Skip all front matter: Jump to Page 1 ▼

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **2014**	2. REPORT TYPE	3. DATES COVERED **00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE **The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **RAND Corporation,Arroyo Center,1776 Main Street, P.O. Box 2138,Santa Monica ,CA,90407-2138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**84**	

The Other Quiet Professionals

Lessons for Future Cyber Forces from the Evolution of Special Forces

Christopher Paul, Isaac R. Porche III, Elliot Axelband

RAND CORPORATION

RAND ARROYO CENTER

The Other Quiet Professionals

Lessons for Future Cyber Forces from the Evolution of Special Forces

Christopher Paul, Isaac R. Porche III, Elliot Axelband

Prepared for the United States Army

Approved for public release; distribution unlimited

For more information on this publication, visit www.rand.org/t/rr780.html

Library of Congress Cataloging-in-Publication Data

Paul, Christopher, 1971-
The other quiet professionals : lessons for future cyber forces from the evolution of special forces / Christopher Paul, Isaac R. Porche III, Elliot Axelband.
pages cm
Includes bibliographical references and index.
ISBN 978-0-8330-5973-4 (paperback : alkaline paper)
1. Cyberspace—Security measures—United States—Planning. 2. Computer networks—Security measures—United States—Planning. 3. Cyberterrorism—United States—Prevention—Planning. 4. Information warfare—United States. 5. United States. Strategic Command (2002-). Cyber Command—History. 6. U.S. Special Operations Command—History. 7. Special forces (Military science)—United States—History. I. Porche, Isaac, 1968- II. Axelband, Elliot. III. Title.

U163.P38 2014
355.3'43—dc23 2014031747

Published by the RAND Corporation, Santa Monica, Calif.

Cover photo by Lawrence Torres III, U.S. Army

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Preface

U.S. special operations forces have a long and storied history and represent a mature, long-standing capability, but one that struggled in the 1970s and 1980s before winning an institutional champion and joint home in the form of U.S. Special Operations Command. U.S. cyber forces represent new but increasingly critical U.S. military capabilities. With the establishment of U.S. Cyber Command in 2010, the cyber force is gaining visibility and authority, but challenges remain. What lessons might the evolution of U.S. special forces hold for the growing U.S. cyber force?

This report was originally written in 2010 and subsequently updated to reflect ongoing changes to U.S. Cyber Command. The research documented here reviews the history and structure of U.S. special operations forces to extract lessons learned that could be applicable to the Army's cyber organizational efforts.

The sponsors of this research, titled "Tactical LandCyber Operations and Capabilities," are the U.S. Army Training and Doctrine Command, Army Capabilities Integration Center, and the U.S. Army Cyber Command. The research was conducted within RAND Arroyo Center's Force Development and Technology Program. RAND Arroyo Center, part of the RAND Corporation, is a federally funded research and development center sponsored by the U.S. Army.

The Project Unique Identification Code (PUIC) for the project that produced this document is RAN136447.

Contents

Figure and Tables

Figure

Tables

Summary

Both special operations forces (SOF) and cyber forces are, at their operating core, small teams of highly skilled specialists (Porche et al., 2008), and both communities value skilled personnel above all else. The SOF community embodies this point in its set of "SOF Truths," originally espoused by COL Sid Shacknow in the mid-1980s:

> Humans are more important than hardware. Quality is better than quantity. Special Operations Forces cannot be mass produced. Special Operations Forces cannot be created after emergencies. (USSOCOM, 2008, p. 29)

These statements also apply to cyber forces, given the high level of skill and training required for such occupations.

SOF represent a much more mature and long-standing capability than cyber forces, but that capability struggled in the 1970s and 1980s before winning an institutional champion and a joint home in the form of U.S. Special Operations Command (USSOCOM). What lessons does the evolution of SOF offer the still-nascent cyber force? Given the role of the U.S. Army in organizing, training, and equipping part of the broader cyber force, what can the Army learn from the experiences of SOF? This monograph attempts to answer these questions by exploring the utility of an analogy between SOF and cyber forces.

The History of Special Operations Forces

Elite commandos of one flavor or another date back quite far in history. The United States' special forces date back to the revolutionary war, and contemporary U.S. SOF can directly trace their lineage to various organizations of World War II. Despite this long history and many storied successes, SOF were historically subject to massive postwar cutbacks and an accompanying deterioration of capabilities. This was due in part to tensions between SOF and conventional forces and in part to the perception of SOF as what Susan L. Marquis has described as *precarious values*:

> Goals or missions within an organization that are in conflict with, or in danger of being overwhelmed by, the primary goals or missions of the organization. Precarious values may be at risk because of a lack of interest by the organizational leadership or because they are in conflict with the primary organizational culture, or sense of mission, or the institution. (Marquis, 1997, p. 7)

After heavy employment in Vietnam, U.S. SOF were once again allowed to decay, limping into the 1980s. Several high-profile failures (Desert One, SOF operations in Grenada) highlighted these shortcomings and demonstrated institutional problems in how the services supported SOF that made improvement unlikely. This led to an acrimonious reform process that involved Congress imposing a new structure for the advocacy and support of SOF: USSOCOM and the Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict.

How Cyber Forces Are Like Special Operations Forces

SOF and cyber forces share similarities that go beyond the fact that both are small teams of "quiet professionals." Pre-USSOCOM SOF and contemporary cyber forces have significant commonalities with regard to their personnel needs, their state of doctrinal development, the strategy for their development as a force, the institutionalization of their training, and their adequacy relative to potential demand. They have further similarities in their relationship to conventional forces, in their applicability across the spectrum of conflict, in their acquisition needs, and in the kinds of reforms called for in support of their respective communities. While there are important differences in other aspects of their personnel needs, the extent of their historical tradition, and their core essences, they have enough in common for the history of the former to be quite informative for the future development of the latter.

How Cyber Acquisition Could Be Modeled After USSOCOM's Rapid Acquisition Approach

The formal U.S. Department of Defense (DoD) acquisition process is complex, consisting of many checkpoints, studies, and subprocesses. The process is designed to meet needs while satisfying requirements, at minimum cost and risk. As a result, it is notoriously slow. Specifically, defense acquisition policy (as specified in the DoD 5000-series documents and the Joint Capabilities Integration and Development System) often results in program execution times—from validation of program need to fielding—on the order of ten years or more (Bennett, 2010). Included in these acquisition efforts is the purchasing of information technology (IT), which DoD recognizes as being too slow to get modern tools into the hands of warfighters (Carden, 2009). This is problematic because IT is the foundation of needed cyber assets. If adversaries can take advantage of the rapid advances in the commercial IT/cyber marketplace, they can leap ahead faster than the U.S. military. Cyber forces require a cyber acquisition pace that is much faster than the formal DoD process.

USSOCOM's Special Operations Research, Development, and Acquisition Center has streamlined the formal DoD acquisition process for urgently needed SOF capabilities. This is allowed because exceptions to the formal DoD acquisition process are permitted under conditions of urgent need. Specifically, USSOCOM has what it calls urgent deployment acquisition (UDA) authority, which facilitates rapid acquisition. It follows a set of guidelines that constrain its application to certain kinds of needs, certain kinds of solutions, and certain timelines.

Many cyber technologies and products have fast development and deployment cycles that must be matched by rapid acquisition to avoid obsolescence when deployed. This process must be couched within broader acquisition strategies and should not be strictly reactive and inefficient, as is sometimes the case with rapid acquisition in wartime. Lessons learned from USSOCOM's rapid acquisition successes should be exploited to enhance cyber acquisition.

Conclusions

Findings suggest that the history of SOF reform, culminating in the 1986 establishment of USSOCOM, has much to offer by way of lessons for a way ahead for the contemporary cyber force, including U.S. Army cyber forces. Pre-USSOCOM SOF and contemporary cyber forces have much in common and many relevant parallels and similarities. The kinds of authorities included in SOF reform that led to today's robust and highly capable SOF community are parallel to the reforms and authorities that could similarly benefit the cyber force. Specifically, we find that, like SOF, the cyber community needs *advocacy* and *a joint organizational home*. Like pre-USSOCOM SOF, it also needs *better funding suppor*t and *a rapid acquisition capability*. However, it is much more dependent on technical acquisition choices at the joint force level. In contrast to SOF, the cyber force needs *nontraditional personnel authorities*.

The establishment of U.S. Cyber Command (USCYBERCOM) will make significant (and perhaps sufficient) strides toward the resolution of the first two needs, for institutionalized senior advocacy and a joint home. Currently, USCYBERCOM is a subordinate unified command under U.S. Strategic Command and does not include any new acquisition or personnel authorities, so further efforts may be necessary to address the final two needs discussed here (a rapid acquisition capability and nontraditional personnel authorities). There remains the possibility of elevating USCYBERCOM to the level of a unified combatant command (not unlike

USSOCOM or perhaps U.S. Space Command) in the future; this notion is supported by the findings presented in this monograph.

Recommendations

This research effort led to several recommendations for DoD and for the U.S. Army. Specifically, we recommend that DoD consider the following steps to foster the capabilities of the U.S. cyber force:

- Empower USCYBERCOM as a joint home for the cyber community.
- Find acquisition solutions for needed cyber tools.

In addition, we offer the following recommendations for the U.S. Army:

- Support USCYBERCOM as a capstone coordinator of and organizational home for the whole cyber force.
- Make Army Cyber Command for Army cyber forces what USSOCOM is for all SOF.
- Recognize the precarious value that cyber forces represent, and support them accordingly.
- Seek nontraditional personnel authorities.
- Reform Army acquisition by modeling cyber acquisition after USSOCOM's rapid acquisition approach.

Acknowledgments

We would like to thank our reviewers, Dennis Murphy, Mark Sparkman, and Susan L. Marquis, for their constructive comments on drafts of this monograph. We also acknowledge the input that we received from personnel at the Ft. Gordon Signal School, the Army Global Network Operations and Security Center, and U.S. Army Intelligence and Security Command (INSCOM) at Ft. Belvoir. In addition, we benefited from frequent interaction with MG Bill Gerety, BG Steven Smith (who now directs the Army Cyberspace Task Force), LTC Hattie Bouyer, and David Shaddrix from the Army G-6. Furthermore, BG Francis Mahon and Timothy Muchmore at the Army Quadrennial Defense Review Office, as well as LTC Robert W. Jones, Jr., and Kenneth Finlayson of the U.S. Army Special Operations Command History Office, provided useful input for our study.

We are indebted to Hugh Stallworth, Anthony Davis, Dave Hodges, Angela Morrell, Barbara Roark, LTC Amy Arwood, and COL Eric Buchannan at USSOCOM, who hosted us on May 13, 2010, and provided invaluable information for this research. We also thank Jean Hurst and Joan Rivera for setting up our visit.

In 2007 and 2008, RAND hosted four workshops on Army cyberspace requirements and policy. Discussions and findings from those workshops contributed significantly to this and earlier reports. Key personnel who led discussions or presented briefs at the workshops included MG (ret.) John Defreitas (INSCOM), COL Wayne Parks (U.S. Army Training and Doctrine Command [TRADOC] Combined Arms Center), LTC Bryant Glando (G-3/5/7, Information Operations Division), LTC Tim Toler (G-2, Operations and Plans Directorate), LTC Robert Butts (Joint Functional Component Command–Network Warfare [JFCC-NW]), Tim Thomas (Foreign Military Studies Office), LTC (ret.) Matt Stern, John Mahony (1st Information Operations Command), John Mense (INSCOM), Paul Schuh (JFCC-NW), Russell Fenton (U.S. Army Network Enterprise Technology Command), and CW5 Todd Boudreau and Mike Muztafago (Army Forces Strategic Command). Finally, we acknowledge the more than 100 attendees who participated in these workshops. Although we are unable to thank all of them individually, their input was critical in guiding this research and refining our approach, and we are grateful for their contributions.

We also had the opportunity to speak with Riley Repko, Joe Thompkins, LTC Terry Torraca, Rickey Smith, Kristen Baldwin, COL Jet Bibler, Tom Curley, Stew Hahn, Jay Kistler, Andy Mellow, LTC Forrest Hare, David Poole, and Jos Olivero about acquisition matters.

More recently, we benefited from engaging discussions with others in TRADOC, including Al Resnick (Army Capabilities Integration Center) and COL Jet Bibler, as well as, on a more recent visit, Tim Thomas (Foreign Military Studies Office) and Jeff Hoing, Bob King, and Tom Jordon (U.S. Army Combined Arms Center, Capability Development Integration Directorate).

At RAND, this research effort benefited from spirited debate and discussions with a number of research colleagues, including Timothy Bonds, Richard Mesic, Myron Hura, Lynn Scott, Martin Libicki, Roger Molander, and John Parachini. David E. Johnson provided direct input from his research on armor development.

We are particularly grateful for the administrative and support efforts provided to us by other RAND colleagues. Diane Vaughn spent much time consolidating input from the research team and formatting early drafts. Michelle McMullen proofread and organized later drafts. We also thank our editor at RAND, Lauren Skrabala, for her patience and attention to detail and general guidance.

Abbreviations

ASD(SO/LIC)	Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict
CINCSOC	commander in chief of U.S. Special Operations Command
CMNS	Combat Mission Needs Statement
CNA	computer network attack
CND	computer network defense
CNE	computer network exploitation
CNO	computer network operations
COCOM	combatant command
DoD	U.S. Department of Defense
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel, and facilities
GWOT	Global War on Terrorism
IA	information assurance
IDIQ	indefinite delivery/indefinite quantity
INSCOM	U.S. Army Intelligence and Security Command
IT	information technology
JCIDS	Joint Capabilities Integration Development System
JFCC-NW	Joint Functional Component Command–Network Warfare

MFP	Major Force Program
NSA	National Security Agency
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OPTEMPO	operational tempo
OSD	Office of the Secretary of Defense
POM	Program Objective Memorandum
SEAL	sea, air, and land
SFG	Special Forces Group
SOF	special operations forces
SORDAC	Special Operations Research, Development, and Acquisition Center
TRADOC	U.S. Army Training and Doctrine Command
UDA	urgent deployment acquisition
USASOC	U.S. Army Special Operations Command
USCYBERCOM	U.S. Cyber Command
USSOCOM	U.S. Special Operations Command
USSTRATCOM	U.S. Strategic Command

CHAPTER ONE

Introduction

Contemporary U.S. cyber forces face many challenges. Current threats in cyberspace are considerable, and attacks are both continuous and ongoing but wholly unlike conventional military operations in methods, scope, and consequences. As an illustration, the following could serve as a cyber force posture statement:

> Our nation is at war, but this war is unlike any we have ever fought. It is a war fought without formal declaration, without concrete resolution, and against adversaries willing and able to circumvent our military forces by striking directly against the U.S. Homeland. It is a long-term conflict against adversaries determined to use weapons designed to cause catastrophic injury to our people and our way of life.
>
> *U.S. cyber forces* are playing a critical role in this war, by bringing terrorists, their supporters, and their state facilitators to justice, or by taking justice to them.
>
> But winning this war will require new capabilities, sustainable increases in capacity, and significant improvements in the global reach and response time of our forces. To meet the demands of the new environment, cyber forces must ensure that their capabilities are well-tuned to meet emerging needs.

The above quotation effectively (and somewhat dramatically) highlights some of the challenges facing the contemporary cyber force. That is not, however, what it was *meant* to do. The above quotation originally referred to U.S. special operations forces (SOF) and comes from a U.S. Special Operations Command (USSOCOM) posture statement (USSOCOM, 2003, p. 27; emphasis in the quotation indicates points of modification). In what appears above, we have replaced references to SOF with references to cyber forces but otherwise left the statement unchanged. The substitution works fairly well: The threats dealt with by contemporary SOF and contemporary cyber forces have much in common, at least at this level of abstraction. What else do SOF and cyber forces have in common? What else *should* they have in common?

Purpose

This monograph explores the utility of an analogy between SOF and cyber forces. Given that SOF represent a much more mature and long-standing capability than cyber, but one that struggled in the 1970s and 1980s before winning an institutional champion and joint home in the form of USSOCOM, what lessons does the evolution of SOF offer the still-nascent cyber force?

Findings suggest that the history of SOF reform, culminating in the 1986 establishment of USSOCOM, has much to offer by way of lessons for a way ahead for the contemporary cyber force. Pre-USSOCOM SOF and contemporary cyber forces have much in common and many relevant parallels and similarities. The kinds of authorities included in SOF reform that led SOF to becoming a robust community and capability are parallel to the kinds of reforms and authorities that could similarly benefit the cyber force. We are not the first to recognize the similarities between SOF and cyber forces or to suggest the applicability of the USSOCOM model to future cyber forces (see Pyburn, 2009). Specifically, we find that, like SOF, the cyber community needs advocacy and *a joint organizational home*. Like pre-USSOCOM SOF, it also needs *better funding support* and a rapid acquisition capability (especially at the service level). However, it is much more dependent on technical acquisition choices throughout the joint force level. In contrast to SOF, the cyber force needs nontraditional personnel authorities.

The establishment of U.S. Cyber Command (USCYBERCOM) will make significant (and perhaps sufficient) strides toward the resolution of the first two needs, for institutionalized senior advocacy and a joint home. Currently, USCYBERCOM is a subordinate unified command under U.S. Strategic Command (USSTRATCOM) and does not include any new acquisition or personnel authorities, so further efforts may be necessary to address the final two needs discussed here (a rapid acquisition capability and nontraditional personnel authorities).

Approach

This analysis relies on comparative case studies: one of the history of U.S. SOF institutionalization through the establishment of USSOCOM and the other of the only partially complete history of the growth and maturation of U.S. cyber forces. The use of historical analogies can be somewhat perilous methodologically (see concerns raised by Khong, 1992, and Record, 1998). Cases that are insufficiently similar can lead to “lessons” whose predicates are not actually available. Care must be taken to establish similarities and differences and to assert only those parallels that are based on genuinely analogous events and relationships. The narrative in this monograph is very careful to make clear the similarities and differences derived from our research effort and to draw only conclusions that are merited. With but two cases to compare, there are no appropriate quantitative methods to ensure or establish similarity or comparability. Instead, this monograph relies on narrative historical methods.[1]

Organization of This Monograph

The remainder of this monograph is organized as follows. Chapter Two details the history of U.S. SOF before the establishment of USSOCOM, including the events that led Congress to take action and establish a separate unified command for SOF. Chapter Three continues the discussion of SOF history by describing the evolution of USSOCOM and its implementation struggles after establishment. This is followed by a brief discussion of the roles for and organization of cyber forces in Chapter Four. ‚Ä®Chapter Five seeks to confirm the validity of our analogy between SOF and cyber forces, enumerating differences and similarities between the two communities and their histories and drawing general lessons learned. Chapter Six takes a closer look at USSOCOM acquisition authorities and draws more extensive lessons for cyber acquisition. Chapter Seven offers conclusions and recommendations.

[1] See the following for discussions of narrative methods: Abbott, 1990; Aminzade, 1992; and Stryker, 1996.

CHAPTER TWO

Special Operations Forces Before U.S. Special Operations Command

The history of SOF and SOF reform substantially precedes the establishment of USSOCOM. Beginning with the early history of SOF "commandos," this chapter briefly reviews the relevant history and some of the details leading up to the SOF reform movement in the 1980s and the establishment of USSOCOM.

The Long and Storied History of Commandos

Elite commandos of one flavor or another date back quite far in history. The occupants of the Trojan horse were no doubt the period SOF equivalent. The United States' special forces predate the country's independence; during the Revolutionary War, the Continental Congress established ten Ranger companies. Famous Ranger leaders from that era included Colonel Daniel Morgan and Colonel Frances "Swamp Fox" Marion.

Contemporary U.S. SOF can directly trace their lineage to various organizations of World War II: the Office of Strategic Services, the air commandos, Scouts and Raiders, and the 1st Special Service Force, for example (Marquis, 1997, p. 4). After the war, however, these robust capabilities were allowed to wither away. All billets, save those for a few navy frogmen and a few air commando pilots, were eliminated. Thus began a worrisome trend in which after each major war or conflict, "U.S. special operations forces—despite their wartime accomplishments and between-the-war usefulness—have been cut back to the bare bones" (Marquis, 1997, p. ix).

Vietnam and Its Aftermath

SOF played a significant role in the Vietnam conflict, and their role substantially expanded during that era. Some of this resurgence was due to President John F. Kennedy's call for the regeneration of nonconventional military capabilities following the 1961 Bay of Pigs fiasco (Marquis, 1997, p. 13).

Despite the prominent role SOF played in Vietnam, Laos, and Cambodia, Kennedy's call for renewal and the persistence of the global realities that had motivated it did not survive that conflict:

> [W]ith the American pullout and force downsizing of the mid-to-late '70s, SOF wallowed at the bottom of the trough. Nearly nine active duty Army Special Forces group equivalents shrank to three, all under-strength, one of which was scheduled for imminent deactivation in 1980. SOF aircraft suffered similar reduction fates or were transferred to the Reserves. The Navy decommissioned its only special operations submarine. SOF manning levels in every Service dropped well below authorized strengths. Funding declined precipitously, amounting to about one-tenth of one percent of the U.S. defense budget by 1975. (Lenahan, 1998, p. 199)

According to Marquis (1997, p. 4), "As late as 1979, army leadership considered inactivating one of the three remaining Special Forces groups, and only 3,600 troops remained assigned to active duty Special Forces units." This period also saw challenges for the naval special warfare community. The SEAL ("sea, air, and land") force narrowly avoided being relegated to the U.S. Navy Reserve (Marquis, 1997, p. 36).

Observers attribute this dramatic deterioration to similar postwar declines in the quality of conventional forces (Marquis, 1997, p. 40), as well as to distrust between the SOF community and the conventional military (USSOCOM, 2008, p. 5) and lack of high-level institutional advocacy for SOF (Boykin, undated, p. 9). Part of the problem was a long-standing cultural disconnect and, in some cases, active dislike for SOF and their activities. "Both Special Warfare and Special Forces were terms that raised many hackles among the conventional regulars" (Boykin, undated, p. 3). This cultural disconnect was compounded by the "blackened" reputation of SOF coming out of the Vietnam War:

> The Special Forces' and other special operators' link with the Central Intelligence Agency gave SOF a freedom in Vietnam that alienated the conventional military. Allegations, and the occasional reality, of such excesses as torture and assassination damned army Special Forces in the eyes of an already suspicious military command and the American people. (Marquis, 1997, p. 20)

Ultimately, it came down to money; as post-Vietnam budgets for SOF withered, so did the force itself.

U.S. Special Operations Forces Limp into the 1980s

Certain individuals understood the value of SOF and fought hard to retain and expand existing capabilities. Some elements in the Army, in particular, managed to develop new (if underfunded, undermanned, and otherwise undersupported) capabilities for counterterrorism. These new entities included the Joint Task Force 7X personnel at Readiness Command, the "Blue Light" Ranger counterterrorism element, and, ultimately, a separate SOF detachment (Lenahan, 1998, pp. 11–20).

Susan Marquis eloquently describes the state of U.S. SOF at the end of the 1970s:

> [A]ll was not well in U.S. special operations forces at the end of the 1970s. The SOF units had survived the decade after Vietnam, but just barely. The SEALs had traded away many of their unconventional capabilities in order to support the fleet. The navy was spending little on SEAL modernization, particularly in support of SEAL tactical mobility. The three remaining army Special Forces groups had little money for training and support and were rarely called upon by military leaders. The 7th SFG [Special Forces Group] had barely escaped being consigned to the U.S. Army Reserves. . . . Funding remained spotty at best. Although funding for special operations improved slightly in the late 1970s . . . it constituted only one-tenth of 1 percent of the total defense budget. At this level, training and operational tempo remained low, tactical mobility was severely limited, and there was no significant SOF modernization program in place. As the 1970s came to a close, the future of the American special operations capability looked uncertain at best. (Marquis, 1997, p. 68)

Heading into the 1980s, SOF airlift was the most glaring of a host of deficiencies. Airlift deficiencies would be exposed and highlighted by the events of Operation Ricebowl and the catastrophe at Desert One.

The Catalytic Failure at Desert One, 1980

In April 1980, Operation Ricebowl infiltrated SOF into Iran in an attempt to rescue hostages taken at the U.S. Embassy in Tehran. RH-53D Sea Stallion SOF airlift helicopters, flown overland after launching from an aircraft carrier, rendezvoused with fixed-wing C-130 Hercules lifters loaded with fuel at a now-notorious site in the Iranian desert: Desert One (Bowdan, 2006). The operation was aborted when an insufficient number of functional helicopters reached Desert One; too few of the birds launched from the carrier were still mission-capable at the rendezvous point. Essentially, there were too few helicopters to ensure adequate redundancy launching from the carrier, which was the result of too few SOF-capable helicopters in the overall

U.S. inventory. Only eight RH-53Ds had been available; all eight had flown from the USS *Nimitz*, only six (the minimum number to safely attempt the operation) arrived at Desert One, and only five were able to continue (Bowdan, 2006). Desert One became infamous not because of the aborted mission but because of the subsequent disastrous collision of one of the helicopters with one of the C-130s, resulting in the loss of both aircraft, the deaths of eight men, and the compromise of the mission.

GEN Carl Stiner, the first commander in chief of USSOCOM (CINCSOC), indicated that the failure of Operation Ricebowl "revealed serious shortcomings in the ability of the United States to equip, employ, and command special operations forces effectively in complex, high-risk operations" (Marquis, 1997, p. 72). General Stiner highlighted several problems: the ad hoc nature of the task force, ambiguous command relationships, inadequate equipment, and the lack of dedicated joint special operations forces (Marquis, 1997, p. 72). Footage on Iranian television of the charred bodies and aircraft at Desert One burned into the American psyche, already wounded by the persistent humiliation of the embassy hostages held in Tehran. Complaints and calls for action abounded, particularly in Congress; something had to be done (Marquis, 1997, p. 3). The mission's failure and the reasons for it revealed these shortcomings—and the horrendous accident gave them publicity. The two together allowed the tragedy to become a catalyst.

The aborted operation provided an unwelcome but critical "wake up call" (Lenahan, 1998, p. 199). The tragedy galvanized congressional attention and emboldened existing advocates in the services and in the Office of the Secretary of Defense (OSD). A coalition of advocates began to coalesce, and changes began to take shape.

The 1980 Holloway Commission investigated the tragedy and reached conclusions similar to Stiner's. One of the committee's major recommendations was the creation of a standing counterterrorism joint task force with permanently assigned staff personnel and certain assigned forces (Lenahan, 1998, p. 199).

Despite congressional attention to SOF issues and the growing strength of the reform coalition, institutional resistance was strong. It came primarily from the services. First, the services, which competed with each other, resisted the surrender of too much of their authority and prerogatives in the name of jointness. Second, the Air Force specifically fought the upgrading of its SOF airlift capabilities (Marquis, 1997, p. 87).

> Time after time, Congress authorized funding for new MC-130 Combat Talons.[1] To be more specific, Congress directed the Air Force to buy more of these special operations airplanes. . . . Every year, the Air Force re-programmed those funds and never bought the additional MC-130s. (Boykin, undated, p. 8)

Service priorities always devalued SOF-related systems, and the budgeting and acquisition system allowed the services to reprogram resources, which they did.

[1] MC-130 Combat Talons are C-130 aircraft modified for special operations and used, for example, to infiltrate and exfiltrate special operations teams and for psychological operations.

Reform and Reconstitution in the Early 1980s

In the wake of Desert One, there was movement in the right direction—just less than Congress and other advocates wanted to see. In 1981, veterans of various SOF coordinating communities (including members from the joint task force that planned, coordinated, and conducted Operation Ricebowl) drafted a "statement of operational needs," outlining functional and organizational requirements for the creation of a meaningful and durable special operations capability (Lenahan, 1998, p. 199). This proposal was well received within the Army and contributed to the foundation for Army SOF reforms in the early 1980s. Reform along these lines in the other services and in the joint community continued to lag.

In fall of 1981, the Army released a proposal to create a joint "Strategic Services Command." This idea originated among the same small group of individuals who had promoted the creation of the SOF detachment and the joint task force that had conducted Operation Ricebowl; it was at least partially based on the statement of operational needs (Lenahan, 1998, p. 201). The core proposition was the integration of various service SOF units into a single national organization capable of global operations (Lenahan, 1998, p. 201). Undoubtedly, this proposal formed the kernel ideas for USSOCOM as ultimately realized.

Air Force and Navy opposition combined to defeat the strategic services command proposal (Boykin, undated, p. 4). Not to be deterred, Army Chief of Staff GEN Edward C. "Shy" Meyer (the principal proponent of the plan) led the restructuring of Army SOF along the lines proposed (Lenahan, 1998, p. 201). This led to the creation of the 1st U.S. Army Special Operations Command at Fort Bragg in 1982 (USSOCOM, 2008, p. 5). To this end, General Meyer combined all Army SOF, both within and outside the United States—including Special Forces, Rangers, civil affairs, and psychological operations units—under the new command.

> Furthermore, the army provided Special Forces with more than 1,500 additional spaces, allowing the activation of the 1st Special Forces Group (SFG) at Fort Lewis and the filling of the undermanned existing SFGs, particularly the 10th. The 1st SFG eventually had one battalion forward-deployed on Okinawa. With these actions and with the establishment of the counterterrorist force in the late 1970s, the Army stepped far in front of the other services in rebuilding a special operations capability. (Marquis, 1997, p. 74)

Thus, 1st Special Operations Command played an important role in coordinating the revitalization and expansion of Army SOF (Stewart, Sandler, and Fischer, 1996). It was the foundation on which the U.S. Army Special Operations Command (USASOC) was built, and it provided the Army with a very effective point of interaction with USSOCOM at its founding (Stewart, 1997).

While leading to continued positive SOF reform in the Army, the failure of the Strategic Services Command proposal to gain traction with the other services left the problem of SOF jointness largely unresolved. SOF advocates in the early 1980s were left with three problems that they believed still needed to be addressed: the problem of cyclical and largely inadequate funding for SOF, the problem of SOF aviation, and the jointness problem (Marquis, 1997, p. 87).

Problems Remain: Grenada, 1983

In October 1983, U.S. forces invaded the tiny island nation of Grenada (see Paul, 2008). The operation included significant SOF employment, particularly of SEALs and Rangers. Operation Urgent Fury was a military success overall but highlighted the extremely limited nature of SOF reform to date (Marquis, 1997, p. 91).

The command-and-control structure proved to be inadequate. There continued to be misunderstandings among conventional force commanders about the capabilities and appropriate uses of SOF, and integrated SOF-conventional force planning was distinctly lacking (Lenahan, 1998, p. 203). In congressional testimony in 1986, retired Army Major General Richard Scholtes, who had commanded the joint special operations task force in Grenada, testified that conventional force leaders misused SOF, resulting in high SOF casualties (USSOCOM, 2008, p. 6).

Though not as dramatic a failure as Desert One, the acute lack of SOF progress evidenced in Grenada drew further congressional ire. Despite commissions, proposals, and new reform initiatives, SOF capabilities were not as robust or as thoughtfully used and supported as Congress wanted.

Further Congressional Pushes and Defense Resistance

Representative Dan Daniel (D-Virginia) was a long-standing advocate of SOF reform on Capitol Hill and first sought to realize congressional preferences by expressing them through personal contacts and nonbinding legislative language, hoping that the military services would make needed reforms on their own (Marquis, 1997, p. 108).

> By 1984 advocates for the special operations forces were becoming convinced that significant reform would not result from bureaucratic guerrilla tactics confined to the Pentagon. . . . The reformers began to think that reform would not come from the inside, but it could be directed from the outside. . . . A few members of Congress quickly became involved in the smallest details of Defense Department special-operations-related policy, organization, and resource allocation. Congress stayed deeply involved for the next five years. (Marquis, 1997, p. 107)

Those advocating SOF reform were repeatedly disappointed by active or passive subversion from within the U.S. Department of Defense (DoD). Congress found that getting reform action was like pulling teeth. Year after year, Congress allocated funding for SOF airlift, and the Air Force faithfully reprogrammed to systems with higher priority to the service. Under considerable pressure from Representative Daniel, Secretary of Defense Caspar Weinberger finally approved the establishment of the Joint Special Operations Agency within the Joint Staff in early 1984 (Marquis, 1997, p. 108). However, the new agency had no operational or command authority of any SOF unit—and no real authority to improve SOF capabilities or policies (USSOCOM, 2008, p. 5).

Internal directives and memos could be (and were) classified and ignored; only when discussion took place in public did any accountability seem to adhere. "Those who hoped the problem of special operations reform would go away could ignore classified directives but had to respond to public challenges" (Marquis, 1997, p. 108). This suggested new tactics to reform advocates: public discussion and writing and formal legislative prodding.

One example of such public advocacy was Representative Daniel's 1985 article in *Armed Forces Journal International*, titled "U.S. Special Operations: The Case for a Sixth Service" (see Boykin, undated, p. 9). Daniel wanted to create controversy to gain the attention of those dragging their feet on reform in DoD and let them know that radical options were under consideration; he clearly hoped that this would catalyze them into fixing the problem internally (Marquis, 1997, p. 121). His core argument, however, is quite telling and remains central to the logic that would ultimately lead to the establishment of USSOCOM. SOF capabilities do not fit within the core philosophy of any of the services, and, thus, the services cannot be relied upon to protect SOF institutional interests, especially where budget prioritization is at issue (Daniel, 1985, pp. 72–74). As Daniel eloquently stated in his article,

> No amount of directive authority—budgetary or otherwise—will overcome the capacity of Service staffs to commit mischief should that be their bent. And, so long as SOF remain outside the Services' philosophical core, the temptation to do so will be near-irresistible. (Daniel, 1985, p. 74)

Ultimately, it became clear to SOF advocates that sufficient reform would not come from inside DoD, and they began to look outside. Reform advocates in both the House and the Senate were fed up with DoD's foot-dragging and began to contemplate strong and binding legislative action. According to Marquis,

> Time was running short for opponents of substantial SOF reform. Beginning in May 1986 the House and the Senate began to take action that could only lead to a dramatic reorganization of U.S. special operations forces. Whether this reorganization would be undertaken by the Defense Department or dictated through

> law was the question. For the Defense Department to maintain some control over the ultimate structure of its special operations forces, it would have to react quickly and with full recognition that marginal changes would no longer suffice. (Marquis, 1997, p. 134)

Congress Takes Decisive Action, 1986

As agitation by SOF advocates increased and time continued to pass without effective SOF reform on the part of DoD, momentum began to build in Congress. On the Senate side, Senator Bill Cohen (R-Maine) joined the fray with an article in *Armed Forces Journal International*, "A Defense Special Operations Agency: Fix for a SOF Capability That Is Most Assuredly Broke" (Lenahan, 1998, p. 207). In May 1986, Cohen introduced his proposal for SOF reform in the Senate as Bill S2453, co-sponsored by Senator Sam Nunn (D-Georgia). In June, Representative Daniel submitted his SOF reform bill in the House (Lenahan, 1998, pp. 208–209). Daniel, Nunn, and Cohen felt growing frustration and shared concerns that the U.S. military was not interested in special operations (USSOCOM, 2008, p. 5). Nunn was particularly frustrated "with the services' practice of reallocating monies appropriated for SOF modernization to non-SOF programs" (USSOCOM, 2008, p. 5).

The Senate bill outlined a new unified combatant command (COCOM) led by a four-star flag or general officer; the House bill proposed a new National Special Operations Agency with a three-star head and its own separate and distinct SOF budget (Lenahan, 1998, pp. 208–209).

The two bills differed substantially, but both went much further than reform opponents in DoD would have liked. ADM William Crowe, Chairman of the Joint Chiefs of Staff, added a third proposal to the mix: a compromise proposal that finally indicated a realization on the part of DoD that Congress was serious about SOF reform. Crowe's proposal included a new Special Operations Force Command headed by a three-star and reporting to the Secretary of Defense through the Joint Chiefs of Staff in the same way that a unified command would (Lenahan, 1998, p. 209). Representative Daniel did not feel that Crowe's proposal went far enough; while it did propose separating SOF from the services, it failed to provide high-level advocacy for budget fights or a separate and protected funding lane for SOF (Marquis, 1997, p. 139). The Crowe proposal became "too little, too late," and Congress forged ahead (Lenahan, 1998, p. 209).

The Cohen bill passed in the Senate, and the Daniel bill passed in the House and went to joint conference in September 1986. Despite the differences between the two bills, those who had prepared them shared one common desire: the development and sustainment of a robust special operations capability for the United States (Lenahan, 1998, p. 210). They hammered out a compromise. "The final bill, attached as a rider to the 1987 Defense Authorization Act, amended the Goldwater-Nichols Act and was signed into law in October 1986" (USSOCOM, 2008, p. 7).

The so-called Nunn-Cohen Amendment

> called for a unified combatant command headed by a four-star general for all SOF, an Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict [ASD (SO/LIC)], a coordinating board for low-intensity conflict within the National Security council, and a new Major Force Program (MFP-11) for SOF (the so-called "SOF checkbook"). (USSOCOM, 2008, p. 7; bracketed text in original)

This was an unprecedented level of congressional involvement in internal DoD matters. The establishment of USSOCOM was the first time Congress had mandated the creation of a military command (Lenahan, 1998, p. 211).

Cohen identified four objectives for the legislation:

> (1) Providing close civilian oversight for low-intensity conflict activities; (2) Ensuring that genuine expertise and a diversity of views are available to the National Command Authorities regarding possible responses to low-intensity conflict threats; (3) Improving interagency planning and coordination for low-intensity conflict, and; (4) Bolstering U.S. special operations capabilities in a number of areas, including: joint doctrine and training, intelligence support, command and control, budgetary authority, personnel management, and planning. (Quoted in Boykin, undated, p. 5)

CHAPTER THREE

The Transition to and Evolution of U.S. Special Operations Command

A major battle had been fought and won, but the war was by no means over. Simply because Congress passed a law did not mean that those opposing the establishment of USSOCOM gave up. Bureaucracy includes an extensive bag of tricks, and the bureaucratic opposition employed many of them in delaying the full implementation of the legislation.

Further Legislation to Force Implementation

Many in DoD who had opposed the various congressional reforms not only accepted their passage but also supported the new command and its efforts (Marquis, 1997, pp. 209–212). Many others, however, continued to harbor resentment at the imposition and continued what resistance and foot-dragging they could. Real or imagined ambiguities in the Nunn-Cohen Amendment provided opportunities for further squabbling and delays in certain aspects of USSOCOM's establishment. Congress was not pleased and ultimately expressed its displeasure with further legislation (USSOCOM, 2008, p. 7).

There were several obstacles between the passage of the Nunn-Cohen Amendment and the full realization of congressional intent. The first was filling the position and establishing the role of ASD(SO/LIC). The second was over controlling and budgeting for SOF resources. The third obstacle pertained to boundaries: Who was part of SOF and thus under the auspices of USSOCOM? Each issue involved its own sequence of struggles, and the first two led to legislative action in pursuit of their resolution.

Irked by congressional intervention, OSD did not make filling the ASD(SO/LIC) position a priority. It was some time before the first candidate was put forward, and that candidate was a noted opponent of the congressional proposals—clearly someone who would not receive congressional confirmation. A second nomination was not soon forthcoming.

> Convinced that the DoD was not going to cooperate, Congress moved forward with additional legislation. In December 1987, Public Law 100-180 was passed

> and directed, "Until the Office of Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict is filled for the first time . . . the Secretary of the Army shall carry out the duties and responsibilities of that office." Secretary of the Army (SECARMY) John O. Marsh thus became the new ASD/SOLIC while retaining his duties as SECARMY. (Boykin, undated, p. 17)

In addition to filling the vacant post, The National Defense Authorization Act for Fiscal Years 1988 and 1989 (Pub. L. 100-180) also directed the Secretary of Defense to publish a charter for ASD(SO/LIC) and gave the CINCSOC head-of-agency authority with regard to the execution of MFP-11 in an attempt to resolve outstanding questions about the processes for SOF funding and acquisition (Lenahan, 1998, p. 212).

Issues surrounding the execution of MFP-11 preceded Pub. L. 100-180, and that law's passage did not resolve them. The Nunn-Cohen Amendment had created MFP-11 to reform SOF funding, but the wording of the law allowed different interpretations, especially when translated into the sometimes-arcane language of the DoD Program Objective Memorandum (POM) and budget cycle (USSOCOM, 2008, p. 22). It was unclear who exactly would control SOF resources and whether the CINCSOC would participate in the programming and budgeting process in the same way as other unified commanders or in some other fashion (Marquis, 1997, p. 208). Congress assumed that it had resolved this issue with the additional clause in Pub. L. 100-180 assigning CINCSOC head-of-agency authority. The next year would see countless memoranda and meetings over the basic issue of whether the legislation required that USSOCOM have program and budget authority (Marquis, 1997, p. 214). Debate over implementation continued within DoD, with five alternatives offered to the Secretary of Defense in an October 1988 memo (Marquis, 1997, p. 219).

Congressional frustration with the delayed implementation increased. Congress escalated its response, printing clarifications in the *Congressional Record*, enacting amendments to the legislation, and threatening to open inquiries and prevent confirmation hearings for posts elsewhere in the department until the issue was resolved (Marquis, 1997, p. 214). Finally, in September 1988, Congress enacted Pub. L. 100-456 (the National Defense Authorization Act for Fiscal Year 1989), which unambiguously directed the CINCSOC to submit a POM directly to the Secretary of Defense and to exercise authority, direction, and control over the expenditure of funds for all forces in the command (Lenahan, 1998, p. 213). This legislation proved sufficiently clear.

> On 24 January 1989, Deputy Secretary of Defense Taft signed a memorandum giving USCINCSOC budgetary authority over MFP-11. Soon afterwards, OSD gave USSOCOM control of selected MFP-11 programs effective 1 October 1990 and total MFP-11 responsibility in October 1991. For the first time, a CINC was granted authority for a budget and POM. (USSOCOM, 2008, p. 22)

In 1989, the focus shifted from money and funding to personnel. There were two ongoing debates (Marquis, 1997, p. 223): First, who was part of SOF and who was not? Second, how much control over SOF manpower would USSOCOM have?

Some units that were typically considered SOF were not immediately transferred to USSOCOM. For example, in the Army, 1st Special Operations Command housed all Army SOF units, including the 1st, 5th, 7th, and 10th Special Forces (Airborne) groups; the 4th Psychological Operations Group, 96th Civil Affairs Battalion; the 75th Ranger Regiment; the 160th Special Operations Aviation Group (Airborne); numerous Army Reserve and National Guard units; and the John F. Kennedy Special Warfare Center and School (USSOCOM, 2008, p. 19). Not all of these units immediately became part of USSOCOM; initially, Secretary Weinberger withheld the active-duty and reserve psychological operations and civil affairs units. Similarly, the Navy sought to withhold U.S. Naval Special Warfare forces, arguing that these forces were inseparably integrated into the fleet (Marquis, 1997, p. 155).

Regarding personnel control, soldiers, sailors, airmen, and marines join one of the military services and receive their initial training. At some subsequent point, they can volunteer for special operations assignments. The services were concerned that they would foot the bill for these forces but then lose all control of their employment and careers (Marquis, 1997, p. 223). USSOCOM ultimately prevailed on both points.

The Bureaucratic Burdens of Administering New Authorities

Although Congress saw its core intentions realized and won a host of new and separate authorities for USSOCOM, the fledgling command was not well prepared to administer all these authorities. In the wake of the Taft memo establishing MFP-11 and granting CINCSOC POM and budget authority, the new command needed to create a new planning, programming, and budgeting process to execute that authority; this proved to be difficult (USSOCOM, 2008, p. 22).

The SOF community needed to develop a bureaucracy to meet its new obligations and manage its new authorities, but SOF culture was not historically keen on bureaucracy. “The transition from a community that has always focused on operational concerns to one bearing these enormous bureaucratic responsibilities was difficult” (Marquis, 1997, p. 166). But USSOCOM was called upon to execute many functions traditionally reserved for the military services: doctrine development, training, provision of forces to the other unified commands, and overseeing its own planning, programming, and budgeting process and POM for resource management (Marquis, 1997, p. 166). These activities were largely outside the core competencies and experiences of SOF personnel.

USSOCOM inherited some bureaucratic capabilities because it was built on the bones of Readiness Command, disestablished to make way for USSOCOM. Readiness

Command, however, had not had the full range of authority provided to USSOCOM, and the new command was not ready to take up all of its authorities at its establishment. It took several years for USSOCOM to build the necessary capacity and procedures, especially MFP-11. Fortunately, old and new allies and other supportive elements in DoD helped ease some of the command's growing pains.

Evolution After the Establishment of U.S. Special Operations Command

The establishment of USSOCOM and the assignment of the capabilities and authorities established by Congress certainly closed an important chapter in the history of SOF development. However, the continued evolution of SOF and USSOCOM potentially offers additional useful insights for future cyber force planning.

GEN James J. Lindsay was the first commander of USSOCOM. He oversaw the establishment of the command and undertook the many tasks necessary to get it functioning. For example, he had to

> organize, staff, train, and equip the headquarters; establish the relationships necessary to discharge its roles and missions; create MFP-11 to ensure SOF controlled its resourcing; build C2 [command-and-control] relationships with the components, work closely with ASD (SO/LIC), and the Theater Special Operations Commands (TSOCs); define worldwide SOF requirements; and plot the future of the command. (USSOCOM, 2008, p. 8)

General Lindsay also had to balance fully executing the authorities of his command while avoiding further alienating the services and those in DoD who had opposed the command's establishment.

Each commander after General Lindsay made slight modifications to the command's mission statement. After the fall of the Soviet Union, demand for SOF capabilities increased, resulting in a higher operational tempo (OPTEMPO) as SOF were deployed for peacekeeping and humanitarian operations (USSOCOM, 2008, p. 12). USSOCOM met these demands with adjustments to acquisition and training strategies but without expanding or altering its authorities or its formal relationships with other COCOMs.

In the wake of the attacks on September 11, 2001, and the launch of the Global War on Terrorism (GWOT), USSOCOM's authorities and relationships *did* change. Secretary of Defense Donald Rumsfeld gave USSOCOM the lead and wanted a single headquarters to have primary military responsibility for GWOT activities (USSOCOM, 2008, p. 14). Traditionally, DoD divided the world into "areas of responsibility" by geographic COCOM. Before 9/11, USSOCOM trained, organized, and equipped SOF, which were then used by the appropriate COCOM; no single

COCOM had the lead for counterterrorism (USSOCOM, 2008, p. 14). Secretary Rumsfeld's 2002 assignment of GWOT responsibility to USSOCOM changed that—and raised several other questions. First and foremost, GWOT responsibility made USSOCOM an operational command beyond its organize, train, and equip roles for SOF and the management of MFP-11. Second, it was unclear what USSOCOM's new authorities would be and how they would now relate to the ground component commanders.

USSOCOM wanted the authority to compel the other COCOMs to recognize its leadership with regard to GWOT plans (USSOCOM, 2008, p. 16). Understandably, the other COCOMs resisted this, preferring to retain their own authority and surrender nothing more to USSOCOM than a need to coordinate, deconflict, or engage in some other permissive form of interaction.

Eventually, USSOCOM commander GEN Bryan "Doug" Brown presented a draft Unified Command Plan to the combatant commander's conference. The plan included language that required USSOCOM to "synchronize" the COCOMs' plans and operations against terrorists. Synchronize was the key term and implied that USSOCOM had the authority to compel other COCOMs to mesh their plans with USSOCOM's (USSOCOM, 2008, p. 16). Although the COCOMs voted eight to one against Brown's proposal, the Unified Command Plan ultimately signed by the President gave USSOCOM synchronizing authority in this area. Now, USSOCOM had generated plans for the GWOT and synchronized other COCOMs' regional plans with its global plan. USSOCOM's global plan would also become the foundation for resourcing plans for the COCOMs' GWOT programs (USSOCOM, 2008, p. 17).

The GWOT also generated a dramatic increase in OPTEMPO for many SOF elements:

> The 11 September terrorist attacks, OEF [Operation Enduring Freedom], OIF [Operation Iraqi Freedom], and the GWOT presented enormous challenges and placed heavy demands on SOF. With each combatant commander requesting more SOF, USSOCOM had to manage the competing demands on the force. To do this successfully, General Brown requested and received authority to manage SOF globally for the GWOT. (USSOCOM, 2008, p. 29)

Before 9/11, COCOMs would submit requests to have SOF deployed to their area, and USSOCOM would provide forces or request relief from tasking on a case-by-case basis (USSOCOM, 2008, p. 29). After 2004, SOF were managed globally rather than regionally, with USSOCOM holding large management conferences and releasing annual posture plans for the growth and employment of the force (USSOCOM, 2008, p. 29).

The Authorities of U.S. Special Operations Command

The three pieces of legislation that codified SOF reform directed four major organizational changes: the establishment of a board for low-intensity conflict at the National Security Council, the establishment of ASD(SO/LIC), the establishment of a COCOM for SOF (USSOCOM), and a separate budget and procurement authority for SOF (MFP-11). What benefits, authorities, and responsibilities did USSOCOM end up with?

USSOCOM, though a COCOM, is unlike the geographic COCOMs in significant ways. At its establishment, it had no designated geographic area of responsibility; now, with the new synchronizing authority for counterterrorism, USSOCOM has a global portfolio, but with functional rather than geographically based responsibilities. USSOCOM is, in many respects, more like a service than a COCOM: It prepares and provides forces for use by the regional COCOMs and has research, development, and POM/budgeting responsibilities (Lenahan, 1998, p. 214).

> The responsibilities of managing MFP-11 and developing and acquiring special operations-peculiar items made USSOCOM unique among the unified commands. These responsibilities—dubbed "service-like"—had heretofore been performed exclusively by the services. Congress had given the command extraordinary authority over SOF force structure, equipping, and resourcing. (USSOCOM, 2008, p. 12)

Unlike a service, however, USSOCOM does not have personnel recruitment and accession authority.

USSOCOM's core mission responsibilities (as enumerated in USSOCOM, 2008, p. 12) are as follows:

- Develop SOF doctrine and tactics, techniques, and procedures.
- Conduct specialized courses of instruction for all SOF.
- Train assigned forces and ensure the interoperability of equipment and forces.
- Monitor the preparedness of SOF assigned to other unified commands.
- Monitor the promotions, assignments, retention, training, and professional development of all SOF personnel.
- Consolidate and submit program and budget proposals for MFP-11.
- Develop and acquire SOF-peculiar equipment, materiel, supplies, and services.

The mission and authorities of USSOCOM provide the SOF community with several benefits. First and foremost, SOF now has a robust institutional advocacy structure. "The establishment of a four-star Commander in Chief (CINC) and an ASD (SO/LIC) eventually gave SOF and voice in the highest councils of the Defense Department" (USSOCOM, 2008, p. 7). With the establishment of 1st Special Operations Command in 1982, the Army had headed down this path, but USSOCOM is a bigger step. Second, the need for constant advocacy for SOF has been reduced. The force is institutionalized in USSOCOM, and the independent control inherent in MFP-11 precludes the SOF community's need to lobby the services or Congress to ensure that its core needs are met.[1] Third, the establishment of USSOCOM ultimately fostered interservice cooperation among SOF units. Having a single commander for the entire SOF community helped promote and ensure interoperability between SOF components from different services in a way that no single-service-led effort could (USSOCOM, 2008, p. 7).

Finally, there are a host of less tangible and quantifiable benefits. According to Boykin, writing in the early 1990s,

> Special operations forces are better off today than in 1986 in many ways. The creation of USSOCOM has had a significant impact on the training and readiness of the special operations forces of the Army, Navy, and Air Force. A renewed pride has emerged at the operational level and quality personnel are more easily attracted to what was previously perceived as a dead-end career path. Joint doctrine and tactics are developed and practiced through routine training and exercises sponsored by USSOCOM. The community had direction and focus, which it lacked in the past. (Boykin, undated, p. 19)

[1] A reviewer correctly noted that SOF must still lobby the services for required standard equipment (equipment that is not "SOF-peculiar"), as well as the COCOMs and the Joint Staff to ensure that SOF are used appropriately.

CHAPTER FOUR

Cyber Forces and U.S. Cyber Command

Before attempting to make an analogy between pre-USSOCOM SOF and contemporary cyber forces and discerning lessons to be learned from the history of SOF, we need to say something about cyber forces and their current state. It is difficult to explore the activities of cyber forces in detail in an unclassified report. As is the case for SOF, the tactics, techniques, and procedures of cyber warfare are classified. Cyber doctrine, such as it exists, is not available for public release and may well be classified in whole or in part. "In fact, the very term *computer network attack* was classified until October 1998 with the publication of JP 3-13" (Armistead, 2004, p. 74). This chapter presents some publicly available foundational information about the roles and nature of cyber forces.

The Lexicon

Some notion of the structure and activities of cyber forces can be gained by examining the unclassified lexicon as embodied in Joint Publication 1-02, the Department of Defense Dictionary of Military and Associated Terms, which contains the following relevant definitions:

> *cyberspace*—A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
>
> *cyberspace operations*—The employment of cyberspace capabilities where the primary purpose is to achieve military objectives in or through cyberspace.
>
> *computer network operations*—Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. Also called CNO.

> *computer network attack*—Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA.
>
> *computer network defense*—Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks. Also called CND.
>
> *computer network exploitation*—Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Also called CNE.
>
> *network operations*—Activities conducted to operate and defend the Global Information Grid.
>
> *information assurance*—Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA.

From these definitions alone, we can correctly infer that cyber forces conduct *cyberspace operations* in *cyberspace*. Such operations include computer network operations (and its three subordinate constructs—attack, defense, and exploitation) and the routine operation and defense of cyberspace implicit in *network operations*. *Information assurance* has a broader reach beyond cyberspace (in as much as information can be stored off the network) but in practice primarily concerns the cyber domain. IA is not equivalent to, but has an important relationship with, CND.

The term *cyber forces* remains officially undefined and open to some debate. At its worst, the category could be too broad. As Andures (2010, p. 118) notes, "It could be argued, after all, that everyone who touches a keyboard, from Servicemember to contractor, is a default member of the cyberspace rank and file." One of the remaining tasks for this community (and presumably a task for USCYBERCOM) is the bounding of the community, including the clear specification of who is in and who is out.

In unpublished RAND research (e.g., Porche, Paul, et al., 2010), we constrained *cyberwarrior* to denote personnel who carry out cyberspace operations, specifically those who perform tasks that are vital for CNO, CND, CNA, or CNE.[1] We further discriminated the latter two activities (attack and exploitation) as network warfare and the former pair (operations and defense) as network operations. This is not the only possible boundary scheme, but it captures the intuition of most experts regarding

[1] A reviewer noted that *cyberwarrior* is used in the U.S. government to describe military personnel, specifically, who perform tasks in support of Title 10 activities. Our working definition makes neither constraint.

U.S. cyber forces. Cyber forces are not those who use the network as part of other activities; rather, they are those who maintain, operate, and defend the network and those who operate in and through cyberspace (as in CNA and CNE).

Cyber Force Roles

A number of broad roles are common to both U.S. military cyber forces and the private sector. These examples are drawn from the U.S. Department of Homeland Security (2008), but we have modified and expanded them based on other draft taxonomies and actual cyber force activities.

- Administrators and technicians
  - Activities: troubleshoot technical problems, install hardware and software
  - Training: operate and repair hardware, configure servers, etc.
- Developers and engineers
  - Activities: design and develop tools, software, and other information technology (IT) to support the organization's activities
  - Training: knowledge of languages and operating systems used; most developers in both private and public organizations have bachelor's degrees in computer science or engineering, with the majority also having master's degrees in related fields
- Analysts
  - Activities: gather information about network performance for forensic purposes
  - Training: usually overseen by the organization; typically, a bachelor's in computer science is a minimum requirement for industry positions
- Acquisition and procurement personnel
- Trainers and educators.

Other roles are more closely aligned with those in military and governmental agencies:

- Planners
  - Activities: mission planning
  - Training: usually overseen by a military training organization
- Operators
  - Activities: carrying out planned missions, both offensive and defensive
  - Training: overseen by the National Security Agency (NSA) and intelligence schools in each service.[2]

[2] A reviewer noted that cyber force training must go well beyond traditional "geek skills." Some cyberwarriors need not only computer language training but foreign language training as well. Further, the cyber force must

Forces for CNA or CNE often take on roles that are traditional to military intelligence forces and not fully detailed in our list.

Some of the possible roles for cyber forces are in tension with other roles. For example, experience has shown that network operator duties and network defense responsibilities should not be assigned to the same dual-hatted person; a cyber/network defender should be singularly focused on protecting against threats and not dually responsible for what can be called network "customer service" (Porche, Paul, et al., 2010). Keeping the network running requires a wholly different set of activities, frame of mind, and tools from those needed to actively monitor the network for evidence of unusual activities and responding to them.

Similarly, there are reported tensions between offensive and defensive military cyber personnel. Institutionally, they have traditionally come from "different worlds," with offensive personnel coming from intelligence units and defensive personnel coming from the military signal community. Beyond just background and organization, CNA or CNE personnel have the highest-level clearances and a culture of secrecy, because sharing a vulnerability could lead others to exploit it or network defenders to attempt to close it, ending its further utility. Network operators and defenders usually have only secret-level clearances and know that closing a vulnerability involves communicating it to others and instituting a change. The best results are possible only when both parts of the force (offensive and defensive) share in a synergistic manner: Defenders need to know the latest offense and exploitation "tricks" if they are to counter them, with similar benefits accruing to cross-trained offensive personnel.

The Need for Uniformed Cyber Forces

Given the substantial overlap between cyber personnel roles in industry and in the U.S. military, one might very reasonably ask whether a government civilian cyber force would be sufficient and whether there is a need for uniformed cyber forces at all. There are at least three arguments for why the United States requires uniformed cyber forces.

Integration into Full-Spectrum Operations

As Starr, Kuehl, and Pudas (2010) report, the Army Concept Capability Plan for Cyberspace Operations outlines a vision for integrating cyberspace into the commander's overall operations. If cyberspace operations are to be a fully integrated part of full-spectrum operations, cyber personnel need to be there, available, part of the chain of command, and part of operations.

include (or have regular access to) personnel with a good understanding of cultural nuances, human dynamics, and influence and persuasion strategies. Cyberwarfare is not always about "0s and 1s"; it can also involve the placement of content on adversaries' networks—content other than computer code that is designed to have an impact in the cognitive domain.

Authority to Operate in Cyberspace

The distinction between uniformed and civilian personnel is vital when it comes to what is allowed by the U.S. Code (e.g., Title 10, which concerns the military, versus Title 50, which concerns national defense). Certain activities require DoD personnel to operate under Title 10, which prohibits them from engaging in other types of activities. Legal boundaries become even more complicated if one imagines "cyberwar" as a stand-alone conflict or as part of broader hostilities. Then, issues arise regarding the law of armed conflict and the status of participants as legal combatants, creating further imperatives for uniformed cyberwarriors.

Deployability

The military deploys, and its networks deploy with it. It only makes sense that network operators and defenders deploy, too. While at certain echelons, deployed cyber forces could be civilians or contractors, at lower echelons, cyber personnel need to be uniformed for the same reasons that the vast majority of personnel at such levels are uniformed: habitual integration into operations, military deployment orders, clear roles in the military chain of command, and the fact that, in a pinch, every soldier is an infantryman.

None of these three justifications requires that all cyber forces be uniformed or that they all be forward-deployed. Indeed, constraints under Title 10 and Title 50 are best satisfied with a force that includes both uniformed and civilian personnel to appropriately execute given authorities, and many CNO functions can (and should) be carried out from remote locations as part of reachback.

Current Cyber Force Structure

The military organizations that house what are now considered cyber forces have grown with the evolution of technology and were conceived prior to contemporary views on the nature of the cyberspace domain. Originally, computers were just another part of communication systems. Subsequently, network operations gave rise to a separate set of organizations, while a host of cyber-related organizations sprang up across "two fiefdoms" (attack and exploitation was one, defense was the other).

These legacy organizations are now being consolidated with the formalization of the cyberspace domain, specifically in USCYBERCOM, U.S. Army Cyber Command, the 24th Air Force, the Navy's Fleet Cyber Command, and Marine Forces Cyber Command.

U.S. Army Cyber Forces

On October 1, 2010, LTG Rhett A. Hernandez assumed command of the U.S. Army Cyber Command/2nd Army at Fort Belvoir, Virginia (U.S. Army, 2010). This new command consolidated existing cyber forces from the Army's Network Enterprise Technology Command/9th Signal Command, Intelligence and Security Command, and portions of the 1st Information Operations Command (U.S. Army, 2011).

> Army Cyber Command provides a unity of command and effort in the synchronization of over 21,000 military, civilian and contract personnel responsible for Global Information Grid Operations; Defensive Cyberspace Operations; and, when directed, Offensive Cyberspace Operations. Army Cyber Command provides Full Spectrum Cyberspace Operations and Intelligence support to U.S. Cyber Command (USCYBERCOM) and in support of Army equities. (U.S. Army, 2011)

U.S. Army Cyber Command is responsible for the operation and defense of all Army networks. In addition, the command conducts cyberspace operations in support of full-spectrum operations and "will develop an Army office of proponency to address all doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) domains related to Army Cyber Command space operations" (U.S. Army, 2011).

U.S. Cyber Command

USCYBERCOM, stood up in 2010, achieved "initial operational capability" on May 21 and "full operational capability" on November 3 of that year (DoD, 2010a). USCYBERCOM is a sub–unified command subordinate to USSTRATCOM; service elements include U.S. Army Cyber Command, the 24th Air Force; the Navy's Fleet Cyber Command, and Marine Forces Cyber Command.

> The command is charged with pulling together existing cyberspace resources, creating synergy that does not currently exist and synchronizing war-fighting effects to defend the information security environment.
>
> USCYBERCOM will centralize command of cyberspace operations, strengthen DoD cyberspace capabilities, and integrate and bolster DoD's cyber expertise. Consequently, USCYBERCOM will improve DoD's capabilities to ensure resilient, reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace. USCYBERCOM's efforts will also support the Armed Services' ability to confidently conduct high-tempo, effective operations as well as protect command and control systems and the cyberspace infrastructure supporting weapons system platforms from disruptions, intrusions and attacks. (DoD, 2010b)

The command continues to develop and grow after achieving full operational capability. Activities have included the establishment of a Joint Operations Center and completion of the transition of personnel from two predecessor organizations, the Joint Task Force for Global Network Operations and the Joint Functional Component

Command for Network Warfare (DoD, 2010b). This transition retains continuity with the prior structure for the coordination of cyber defense.

USCYBERCOM has and will continue to have a very close relationship with the NSA. The two organizations are colocated and share a single commander and director, GEN Keith Alexander. At his nomination hearing before the Senate Armed Services Committee, Alexander described the planned relationship as follows:

> [W]e will have a unique set of authorities, a unique staff for Cyber Command operating under Title 10, and the National Security Agency, Central Security Service under Title 50. We do have some Title 10 responsibilities. We are a combat support agency. We do forward deploy people to help the combat, the regional combatant commanders. But there will be two distinct staffs, with distinct authorities and responsibilities for how we operate for intelligence, for information assurance on the NSA side, and for Cyber Command how we defend and secure our networks and conduct cyber space operations if directed. (U.S. Senate, Committee on Armed Services, 2010, p. 32)

The NSA is the "big dog" on the cyber block, as its long-standing mission set includes cryptology, encompassing both signals intelligence and IA, and enabling CNO (NSA/CSS, 2011). Having developed cyber capabilities as part of its long-standing, preexisting mission set, the NSA is currently the most significant repository for cyber expertise and tools in the U.S. government. It represents a significant enabling resource for military cyber forces through its relationship with USCYBERCOM.

USCYBERCOM has an ambiguous relationship with the military services, however. Tensions persisted and the relationship continued to struggle for clarity at the time of this writing, and these challenges are likely to continue in the future. What is unambiguous is that the military services currently have a Title 10 "organize, train, and equip" obligation with regard to their cyber forces (just as they do for all other forces provided to them). It is not yet clear how much USCYBERCOM will share in those responsibilities and whether USCYBERCOM's role will be supervisory (oversight and specification of requirements), formative (directing career paths, course development, and acquisitions), a partnership (providing some training and tools directly), or some combination thereof.

Also uncertain is how the services will decide which forces will be committed to USCYBERCOM and which will be "retained" at the service level. That is to say, USCYBERCOM has a certain number of joint billets that each service is responsible for filling (and will certainly fill). However, the services retain responsibilities of their own with regard to the cyber domain (such as operating and defending their own networks) and thus must retain a certain portion of the cyber forces they organize, train, and equip. How this will be handled is currently an open question. We have heard anecdotally that different services currently envision different solutions, but no further details were available as of this writing.

USCYBERCOM also has ambiguous future relationships with the COCOMs. It is a subordinate command with responsibility for centralizing the command of DoD cyberspace operations, and it is not yet clear exactly how that role will interface with the geographically bounded responsibilities of the COCOMs. Several models have been proposed, including one resembling USSOCOM's GWOT responsibilities (Birdwell and Mills, 2011). As of this writing, each of the COCOMs had chosen to organize and staff for cyber operations somewhat differently. The current element of commonality is that USCYBERCOM has placed an O-6 liaison officer at every COCOM.

With a better understanding of the nature, roles, and highest-level organization of current U.S. cyber forces, the next chapter compares pre-USSOCOM SOF with contemporary cyber forces to assess the validity of our analogy between them. We also offer additional details about contemporary cyber forces as necessary to highlight points of comparison and contrast with SOF.

CHAPTER FIVE

Confirming the Analogy: How Alike Are Pre–U.S. Special Operations Command Forces and Contemporary Cyber Forces?

The history leading to the establishment of USSOCOM offers important general lessons, including the noted difficulty of garnering support and funding from the services for elements that they do not consider to be a priority, the acrimony engendered by congressional imposition in areas traditionally seen as the prerogatives of the defense community, the power of bureaucratic resistance from those alienated by the process, and the effectiveness of a new organization with high-level advocacy and budget authority for the community it supports. Further lessons may be drawn from an analogy between SOF and cyber forces, but they would be contingent on actual likeness between pre-USSOCOM SOF and (in this case) contemporary cyber forces. This chapter compares the pre-USSOCOM SOF community to the nascent cyber community and notes their common features, the ways in which they are similar, and the ways in which they differ.

Common Features

Pre-USSOCOM SOF and the contemporary cyber force certainly have enough in common to support our analogy. This chapter identifies six features that the two forces share: certain aspects of their personnel (and the careers available to them), the state of development of their doctrine, their organization as communities, the strategies (or lack of strategies) for their development, the extent to which their training is formally institutionalized, and their inadequacy in the face of potential demand. We discuss each point in turn.

Personnel

Both SOF and cyber forces are, at their operating core, small teams of highly skilled specialists (Porche et al., 2008), and both communities value skilled personnel above all else. The SOF community embodies this point in its set of "SOF Truths," originally espoused by COL Sid Shacknow in the mid-1980s:

> Humans are more important than hardware. Quality is better than quantity. Special Operations Forces cannot be mass produced. Special Operations Forces cannot be created after emergencies. (USSOCOM, 2008, p. 29)

The same principles apply to cyber forces. In an article published in *Army Magazine*, Doty and O'Connor (2010, p. 12) echo the importance of "recruiting and building cyberwarfare teams composed of highly talented and skilled individuals."

Another commonality in the area of personnel is the lack of career fields and opportunities for advancement (Porche et al., 2008). The pre-USSOCOM SOF community lacked career fields, as does the contemporary cyber force. While the Navy did have a special warfare branch, the Army lacked an SOF branch until 1987 (Marquis, 1997, p. 41). Anecdotes of promotion-related disadvantages attending early SOF service abound. Many officers understood that, to have any kind of career, they needed to bounce back and forth between SOF and "real" units, because command roles in SOF units did not "count" toward promotion (Marquis, 1997, p. 41).

The contemporary cyber force appears to face the same type of challenge:

> Disadvantaged assignments, promotions, school selection, and career progression for those who pursue cyberwarfare expertise, positions, and accomplishments. Some cyberwarfare soldiers, sailors, and airmen who seek to make a career of the military go to great lengths to mask their technical expertise and assignments from promotion boards by making their personnel evaluations appear as mainstream as possible. (Conti and Surdu, 2009, p. 16)

In the case of SOF, "Careers were made and promotions received for service on navy ships, battalion command, or flying jets" (Marquis, 1997, p. 41), and this remains largely the case for those who consider cyber force careers.

This need to transition back and forth between conventional assignments and SOF or cyber roles created and continues to create, respectively, a lack of career continuity. This pattern carries important consequences because many skills, especially technical skills, atrophy quickly (Conti and Surdu, 2009, pp. 16–17).

Doctrine

Irregular warfare and SOF doctrine lagged operational activities after the Vietnam War and prior to the establishment of USSOCOM. Only with the establishment of USSOCOM has SOF doctrine become in any way robust and current. Current cyber doctrine lags operational realities as well. Some of this is no doubt due to rapid changes in the technology and threats facing the cyber force, but some is due to the same kinds of neglect faced by pre-USSOCOM SOF. In his nomination hearing, USCYBERCOM commander GEN Keith Alexander stated that "we can stand up the command under existing authorities, but there is undoubtedly much uncharted territory in the world of cyber policy, law and doctrine" (U.S. Senate, Committee on

Armed Services, 2010, p. 10). The establishment of USCYBERCOM has not (yet) resolved these challenges. A 2010 *Joint Force Quarterly* article (Andures, 2010) accuses USCYBERCOM of skipping the doctrinal preamble and going straight to organization without setting priorities or establishing a sufficient basis for the marshaling of forces.

Organization

While we refer to the pre-USSOCOM SOF "community" and the contemporary cyber "community," these are not organizationally defined and bounded entities. Early SOF and contemporary cyber "cylinders of excellence" were and are scattered across the services. Disparate formations of pre-USSOCOM SOF met (if they did) when operating or training together, never really convening as a community. U.S. cyber forces are the same; they constitute a community only in that they have common tasks and convene at conferences, through ad hoc working groups, and in other venues. This may change as USCYBERCOM matures and establishes routine patterns of interaction and operation. Whether the command creates a cyber community analogous to the one that USSOCOM created for SOF remains to be seen.

Development Strategy

Both pre-USSOCOM SOF and contemporary cyber forces share a development strategy—that is, not much of one. Both work (or worked) within existing unit frameworks in the services and with the goal of aligning development needs and larger service priorities (Porche et al., 2008). The pre-USSOCOM naval special warfare community, for example, was able to secure its development and sustainment by closely aligning itself with core fleet objectives, including providing indispensible services, such as hydrographic reconnaissance (in support of the Navy's amphibious mission), other special reconnaissance, and taking direct action in support of fleet objectives while abandoning specialties in riverine operations, counterinsurgency, or nation-building (Marquis, 1997, pp. 66–67). Cyber forces have also grown in fits and starts, with development strategies (such as they are) generally confined to single organizations. According to Pyburn (2009, p. 13) the services "are developing cyberspace capabilities in accordance with their respective doctrine and requirements without significant oversight or standardization."

Institutionalization of Training

Formal institutionalization of training lagged for SOF and is lagging for the cyber force. While various SOF schoolhouses were established prior to USSOCOM, they came about fairly late in the history of SOF and lacked joint control and advocacy until they were consolidated under USSOCOM. The cyber community has experienced similar delays. The Army's School of Information Technology at Fort Gordon, Georgia, may mature into a proper "cyber" schoolhouse, but it currently teaches a variety of

IA- and security-related courses that focus primarily on "running" cyberspace rather than "operating inside it."[1] Similarly, the Air Force aspires to make its information operations training facility in Hurlburt Field, Florida, a proper "information operations and cyber schoolhouse" (Kessler, 2010), and the Navy's Center for Information Dominance offers cyber-related training (U.S. Navy Center for Information Dominance, undated), but neither facility is exclusively dedicated to the cyber force or fully established as a cyber schoolhouse.

Adequacy Relative to Potential Demand

The tragedy at Desert One demonstrated that pre-USSOCOM SOF capabilities were not adequate to meet demand, particularly with regard to SOF airlift. While there has been no equivalent humiliating failure for the cyber force, the often-publicized fear of a "digital Pearl Harbor" and the anticipated inadequacy of contemporary cyber forces to meet that challenge suggest that this is another feature likely shared by the two forces (Berinato, 2003).

Similarities

In addition to the common features described in the previous section, pre-USSOCOM SOF and the contemporary cyber force have a number of similarities. The similarities are shared features, but they are not shared as closely. Similarities between the two communities include other aspects of their personnel and personnel systems, their relationship with or to conventional forces, their existence as "precarious values" in a military enterprise whose traditional focus is conventional warfare, their applicability across the spectrum of conflict, their acquisition needs, and the calls for reform made on their behalf.

Personnel

The previous section noted several common characteristics of SOF and cyber personnel and careers. There are additional points of similarity in the personal and personnel management of the two communities. In terms of development, both cyber and SOF personnel require extensive skill sets that take time and practice to acquire and maintain. As mentioned earlier, SOF skills are primarily military-specific, while cyber skills are often available in the private sector. Both SOF and cyber forces seek to develop professionalism and competence; the similarity ends when SOF development also seeks to "increase tolerance and endurance, as well as enhanced performance, sustainment and alertness" (USSOCOM, 2003, p. 65).

[1] Author interviews with personnel at the U.S. Army School of Information Technology, Ft. Gordon, Georgia, April 14, 2010.

Both pre-USSOCOM SOF and contemporary cyber forces have struggled with retention, but for slightly different reasons. Traditional SOF retention issues stemmed from the difficulty of building a successful career primarily in SOF because of the lack of advancement opportunities and "appropriate" command credit. This, coupled with the exacting physical requirements of SOF service, weighed against the extreme loyalty and esprit de corps of SOF to create retention concerns. In the cyber force, retention issues stem first from the lack of institutional regard (and promotion opportunities) for technical experts, but also from the fact that there are extremely lucrative parallel opportunities in the private sector. "As a result, the Army, Navy, and Air Force hemorrhage technical talent" (Conti and Surdu, 2009, p. 15).

Relationship with and to Conventional Forces

Pre-USSOCOM SOF and contemporary cyber forces are similar with regard to their relationship with and to conventional forces. The two communities support conventional operations but are not well understood by conventional operations forces, have their own cultures, and conduct activities that are not conventional operations. "Special operators do not do what conventional forces do, and they do not think the way conventional forces think" (Marquis, 1997, p. 46).

Prior to the establishment of USSOCOM and the clarification of SOF roles, special operations were not well understood, or particularly well regarded, by conventional forces. As LTG Samuel V. Wilson noted,

> There is a cultural aversion on the part of conventional soldiers, sailors, and airmen to things that smell of smoke and mirrors and feats of derring-do. . . . It's a little too romantic. . . . It's not doing it the hard way. . . . Most of the people who have made their rank as battleship and bomber drivers, tank riders, and so on, just don't see this as the main way to go. (Quoted in Marquis, 1997, p. 6)

While the relationship between cyber forces and the conventional military is nowhere near as toxic as that between SOF and conventional forces at one time, cyber force activities are not particularly well understood by conventional forces. While many personnel may understand the objectives of CND and respect the value of secure networks, they are unlikely to have much appreciation for the actual conduct of such operations. Most, however, fail to understand the true extent of threats to the network, and CNA and CNE are even less well understood.[2]

The distinct organizational culture of SOF is often noted in the literature (see, e.g., Marquis, 1997, p. 44). A culture that values independence, critical thinking, and individuality and that lacks undue regard for rank can clash with one that values con-

[2] For example, Col Rich Moorehead, formerly of the Air Force's 57th Information Aggressor Squadron, explained to us that he personally had almost no understanding of the real extent and nature of the cyber threat until he himself became an information aggressor, adding that his was a common experience (Moorehead, 2010).

formity and a nearly unquestioning following of orders. Similarly, aspects of conventional military culture are not core values of the cyber force. Attributes that are highly regarded in the conventional military, such as marksmanship, strength, or precise vehicle maneuvers, are not critical to the cyber force, and impressive technical feats are not held in particularly high regard by line forces. "The cultures of today's military services are fundamentally incompatible with the culture required to conduct cyberwarfare" (Conti and Surdu, 2009, p. 16).

These cultural differences stem directly from operational differences. SOF employ unique operational modes and techniques and require exceptionally detailed intelligence, as well as greater levels of physical and political risk, than is the case in the conventional force (USSOCOM, 2003, p. 7). Cyber operations differ substantially from conventional operations, but in different ways. Conti and Surdu explain that conventional forces

> operate in the kinetic arena, the directed application of physical force, whereas cyberwarfare exists in the non-kinetic world of information flows, network protocols, and hardware and software vulnerabilities. (Conti and Surdu, 2009, p. 15)

"Precarious Values"

In the words of Marquis (1997), SOF and—in our analogy—cyber capabilities are "precarious values":

> goals or missions within an organization that are in conflict with, or in danger of being overwhelmed by, the primary goals or missions of the organization. Precarious values may be at risk because of a lack of interest by the organizational leadership or because they are in conflict with the primary organizational culture, or sense of mission, or the institution. (Marquis, 1997, p. 7)

Marquis goes on to argue that SOF were most definitely a precarious value in the period prior to the establishment of USSOCOM. The SOF community struggled in this role because it lacked protection, in the form of either institutional advocacy or a strong external patron (Marquis, 1997, p. 8).

Cyber forces share this precarious-value relationship with SOF, at least to some extent. Although core cyber missions support primary military organizational goals and cyber forces are unlikely to be subject to the same kind of active resistance, they *are* in danger of being overwhelmed (or overlooked) by services with other priorities. At the level of individual commanders, most may recognize the dependence of command and control and thus successful CND and IA, but they do not necessarily fully understand the requirements of cyberwarfare and will almost always push for access over security if access appears to make their job easier.

To their benefit, cyber forces are not actively disliked either institutionally or individually within the conventional force and now have the centralized advocacy of USCYBERCOM. The command and its close relationship with large and well-funded NSA (where cyber is not a precarious value) protect the cyber force at the joint level. However, as long as Title 10 responsibilities to organize, train, and equip cyber forces remain with the services, cyber forces risk precarious-value status at that level. Paradoxically, the strong relationship between USCYBERCOM and the NSA could increase the risk at the service level, with service decisionmakers declining to prioritize cyber-related resource allocations, assuming that NSA and USCYBERCOM will pick up the slack.

Applicability Across the Spectrum of Conflict

SOF operate across the conflict spectrum, from peacetime engagement to high-intensity combat (USSOCOM, 2003, p. 63). While cyber forces conduct a different and narrower range of operations, those operations also apply across the full range of the spectrum of conflict. As a further note of difference, while cyber forces operate across the spectrum of conflict, they do so in their own distinct domain, the cyber domain, while SOF share the land, sea, and air domains with conventional forces.

Acquisition Needs

Both SOF and cyber forces place a premium on quality personnel, as noted earlier. However, both have a certain degree of dependence on equipment or systems. The SOF operator depends on land, air, or sea insertion systems to access the target area and could certainly benefit from additional personal equipment. Similarly, a cyber operator is useless without a computer of some kind and requires specialized hardware and software for some of the activities in the cyber portfolio.

The systems dependence of SOF is well recognized in the articulation of the need for "SOF-peculiar equipment," the acquisition of which is the raison d'être for MFP-11. Pre-USSOCOM SOF had to rely on the services to program and procure this equipment and often saw these needs go wanting (SOF airlift being the paradigmatic example).

Similarly, cyber forces need to acquire cyber-peculiar equipment, though not at the same programmatic scale as major systems, such as airframes or submersibles. Future cyber forces will require new tools to expand upon or replace existing ones, as well as automated tools that can increase the effectiveness of human operators.

Additionally, cyber forces depend on the computer and network acquisition choices of the broader force. While CNA and CNE may require certain specific equipment, IA and CND are heavily driven by the defensibility of the computers and software that constitute the networks that cyber forces are called upon to defend.[3] SOF face a similar challenge. When looking to acquire SOF-peculiar vehicles, considerable cost savings can be realized by modifying an existing military system to meet SOF requirements, rather than investing in the development of a wholly new platform (Martinage, 2009). USSOCOM acquisitions "rely on service-common equipment and leverage the services' materiel solutions whenever feasible" (USSOCOM acquisition and procurement executive James W. Cluck, quoted in McKaughan, 2009).

MFP-11 suffices for the development and acquisition of SOF-peculiar equipment, and something similar would sufficiently support the need for cyber-peculiar equipment. What a similar funding program alone would not do is meet the broader desires of the cyber force for increased securability of non–cyber-peculiar equipment, i.e., computer and network equipment that is not unique to the cyber force but is used for connectivity by a wide range of joint force elements.

Both SOF and cyber forces require speed and agility in acquisition. MFP-11 rapid acquisition strategies have resulted in the ability "to field a material solution many times faster than traditional aircraft acquisitions" (Anderson, 2008, p. iv). The constant incremental progress at the "bleeding edge" of computer technology makes rapid acquisition even more of an imperative for the cyber force. ADM Eric Olson's description of SOF needs has clear application in the cyber domain, too:

> Ensuring they have the equipment, sensors, weapons, and mobility platforms of the kind and quality demanded by their peculiar missions requires willingness to invest in the rapid fielding of both existing solutions and cutting edge technologies even when the relatively small purchase quantities do not optimize production costs. (Olson, 2008, p. 2)

To some extent, USSOCOM owes its rapid acquisition capability under MFP-11 to its Combat Mission Needs Statement (CMNS) process (Anderson, 2008, p. 12). The CMNS allows operators to identify urgent materiel needs and to have the need validated quickly and turned into an urgent deployment acquisition (UDA). UDAs potentially allow a solution to be fielded in as little as seven days from the approval of the CMNS when a solution is already available in the commercial marketplace (Anderson, 2008, p. 12). Further details on cyber acquisition needs and USSOCOM acquisition solutions can be found in Chapter Six.

[3] If such equipment or software contains inherent vulnerabilities, cyber defenders are left trying to contend with those vulnerabilities after the fact. Further, incautious acquisitions in the broader force include the risk not just of unintended or accidental vulnerabilities in the systems acquired but also of intentional vulnerabilities introduced in such systems. Consider, for example, the risk of embedded malware, in which a software or hardware vulnerability has been intentionally introduced somewhere in the development, production, or delivery supply chain and can be exploited by an adversary in the future.

Calls for Reform

Before USSOCOM, the services failed to answer the needs of the SOF community. In the cyber community, perhaps this path can be avoided. The establishment of USCYBERCOM may lead to further reforms and create sufficient cyber advocacy to encourage an adequate level of commitment on the part of the services to cyber force development and sustainment.

Unsurprisingly, given the many commonalities and parallels between the challenges faced by pre-USSOCOM SOF and contemporary cyber forces, the proposals for reform often have much in common, too. Consider, for example, Representative Dan Daniel's 1985 call for a sixth service for SOF and Conti and Surdu's 2009 advocacy for a sixth service for cyber forces. Beyond the headline-grabbing recommendation (to launch a sixth service), the motives and justifications for these calls for radical reform have important similarities.

Marquis (1997) summarizes several key motivations behind Daniel's (1985, pp. 72–74) proposal: "philosophy" as a way to highlight the differences between conventional force and SOF culture, mindset, and way of doing business; "professionalism" as a call to put an end to reduced career and promotion opportunities for those who chose to join SOF; "budgets," because SOF-peculiar equipment had been forced to unfairly compete for funding with M1 tanks and F-16 fighters; "continuity" to highlight the historical abandonment of SOF forces after major conflicts, regardless of their contributions to those conflicts; "unique solutions to unique problems" to highlight the difficulty of preserving low-density low-demand capabilities while SOF resided in the services; "advocacy" as a reminder that SOF were not a top priority in any service and lacked a formal or institutional advocate; and "relationship with the National Command Authority," echoing another factor related to advocacy, high-level representation.

Conti and Surdu's argument for a cyberwarfare service branch follows similar logic: Akin to Daniel's "philosophy" is their assertion that "the cultures of the Army, Navy, and Air Force are fundamentally incompatible with that of cyberwarfare" (Conti and Surdu, 2009, p. 15). Like Daniel's "professionalism," they note the failure of the services to recognize and develop technical expertise, and the "disadvantaged assignments, promotions, school selection, and career progression for those who pursue cyberwarfare expertise" (Conti and Surdu, 2009, p. 16). While they do not explicitly base their argument on anything analogous to Daniel's "budget" concern, they parallel his argument regarding "continuity" by noting the costs associated with NSA training for junior or midcareer troops who then fail to reenlist or are assigned to other areas in the joint force (Conti and Surdu, 2009, pp. 16–17). Similar to Daniel's point about "unique solutions," they remark,

> Cyberwarfare requires unique technical skills as well as skills in creative problem solving, poise under pressure, and critical thinking. Attributes that are desirable in soldiers, such as physical endurance, marksmanship, and technical skills associated

> with the employment of traditional forces and weapons systems, do not translate well to cyberwarfare. (Conti and Surdu, 2009, p. 17)

While not explicitly calling for "advocacy" or "National Command Authority access," Conti and Surdu do assert that the services value traditional and conventional warfare capabilities and have not and will not structure themselves to reward and encourage the kinds of feats and capabilities that a cyberwarfare force should take pride in.

Both Daniel's and Conti and Surdu's calls for a sixth service are at least equal parts attention-grabbing headline and serious proposal. While these authors certainly recognized the low prospects for a new service, the logic and framework invoked by their arguments ring true and suggest challenges that must be addressed before reform can be successful.

In the 1980s, the Army reorganized its own SOF and designated SOF a "branch." The extent to which the establishment of USCYBERCOM and the various reforms in cyber structures in the services will satisfy the previously discussed motives for reforms remains to be seen (Lord, 2009; Shachtman, 2008; Jackson, 2009).

Differences

There are some significant differences between pre-USSOCOM SOF and the contemporary cyber force. These differences suggest something other than perfect correspondence in the analogy between SOF and cyber forces and indicate that alternative approaches to some of the contemporary challenges may be appropriate. These differences include some aspects of the personnel and personnel systems, differences in age and historical tradition, the effect of specific historical events, and a difference in core essence.

Personnel

Although pre-USSOCOM SOF and contemporary cyber forces exhibit many commonalities and similarities with regard to personnel and personnel management, there are some interesting and important differences. These include the core capabilities of the two forces, how they can and should recruit, and their respective accession paths.

Fundamentally, SOF and cyber force personnel are different. SOF forces are commandos, one and all, and cyber operators are not. SOF have the most admirable features of other types of warfighters: strength, endurance, marksmanship. Cyber forces need and value an entirely different set of skills, including unique technical skills and other "geek arts." Further, on an individual level, SOF are incredibly versatile, combining individual fitness and combat skills with a host of language, cultural, survival, and technical expertise (USSOCOM, 1996, pp. 2–30). Cyber forces do not have (or need) such individual versatility. In fact, the community is currently divided between those tasked primarily with CND and those who focus on CNA or CNE, and the necessity (or wisdom) of cross-training in these disciplines has been debated.[4]

In part because of these differences in the respective skills and capabilities required for SOF and cyber forces, their optimal recruiting pools differ substantially. The military is the preponderant source of personnel for SOF. Many skilled uniformed personnel want to join SOF, and recruitment to these elite forces is a filter function. Civilians who wish to join SOF units willingly join the conventional military and then seek SOF billets.

In contrast, for cyber forces, the best reservoir of preexisting relevant skills is in the civilian workforce. Cyber forces are recruited within the services, too, but many fewer clamor to join the cyber force than is the case for SOF. Further, many fewer civilians who are potentially elite cyberwarriors are inclined to join the military in the first place.

Another difference is force accession. The demanding SOF selection process means that many SOF candidates fail to become SOF warriors (USSOCOM, 2003, p. 65). Cyber forces are not as exclusive nor as elite as SOF; they do not have (and should not have) SOF's 40- to 80-percent attrition rate during selection. Those who show an interest and aptitude for cyber specialties need to be separated from those who do not. There is still some attrition in cyber training, but cyber force accession remains less of a concern than SOF accession.

These different recruiting and accession needs and processes suggest that different recruiting and accession authorities are needed for the cyber force.

Historical Tradition

Unconventional warfare forces and SOF have a long and storied history. The military's cyber force, on the other hand, is genuinely new. SOF's history of strained relationships with conventional forces and the gutting of SOF that occurred after every major conflict prior to the establishment of USSOCOM are historically validated. The cyber force lacks such a tradition.

Salient Historical Events

The sometimes-unfortunate benefit of having a significant history is the ability to point to salient events in that history as justification for reform. Despite playing a critical wartime role, SOF experienced repeated postwar reductions; SOF were subject to cultural marginalization and had their reputations "blackened" by Vietnam; and they

[4] A reviewer asserted that a good cyber defender understands cyber offense, which is certainly true. Discussions with operators, however, have suggested that those who successfully engage in network defense have different intuitions and mindsets than those who focus on offense or exploitation. Training personnel with whom we spoke also indicated that some of the most gifted cyber defenders they had trained were very uncomfortable when posted to a position involving offensive tasks, and vice versa.

endured the catalytic but publicly humiliating tragedy at Desert One. Cyber forces, on the other hand, have had none of these experiences. Any acrimony over cyberspace operations or reform agitation has remained relatively submerged; the community has not yet experienced an "electronic Pearl Harbor" and does not operate in the aftermath of a truly high-profile catastrophe. If it can learn from the challenges faced by pre-USSOCOM SOF, perhaps the cyber community can mature and receive the support and reforms it needs without accruing an unfortunate salient history. Alternatively, it is possible that cyber threats will not be taken seriously or that sufficient capability will be developed to effectively counter them until there is some sort of truly catastrophic, catalytic event.

Core Essence

SOF and cyber forces differ in their core essences. Not only that but their essences are differentially unitary.

An unpublished 1998 RAND study for USSOCOM identified the SOF "telos" or essence: At their core, all SOF are commandos (Peters and Dewar, 1998, p. ix). The authors also articulated a vision for SOF:

> Commandos, ready to respond rapidly to the nation's strategic emergencies that lie beyond the reach and means of conventional military forces. (Peters and Dewer, 1998, p. ix)

Cyber forces do not have such an unambiguous telos or vision. While one might construct an essence statement that has something to do with the cyber domain, the fact remains that the actions and mindsets of personnel who engage in CND are substantially different from the actions and mindsets of who focus on CNA and CNE. To mature as a community, the cyber force needs a joint vision and, perhaps, a more unitary articulation of its telos or essence. Time will tell if USCYBERCOM will provide this. If it can, it should be encouraged to do so.

Table 5.1 summarizes the commonalities, similarities, and differences between pre-USSOCOM SOF and contemporary cyber forces discussed in this chapter.

Lessons from the Analogy

While some important differences separate pre-USSOCOM SOF and contemporary cyber forces, they have enough commonalities and similarities that we can draw lessons from the evolution of the former that have important implications for the future of the latter. Because of their differences, it is necessary to scrutinize each lesson to ensure that it stems from shared factors and not from points of difference.

The history of the establishment of USSOCOM provides both positive and negative lessons. Fundamentally, the destination (an independent organization with its own

Table 5.1
Summary Comparison of Special Operations Forces and Contemporary Cyber Forces

Features	Pre-USSOCOM SOF	Cyber Forces
Commonalities		
Personnel	Small units of highly skilled specialists; lack of career fields, opportunities for advancement, career longevity	Small sets of highly skilled specialists; lack of career fields, opportunities for advancement, career longevity
Doctrine	Doctrine development lagged operations	Doctrine development lags operations
Organization	Scattered across the services; common tasks and ethos but not an organizationally defined community	Scattered across services; common tasks and ethos but not an organizationally defined community
Development strategy	Work with existing units from various services	Work with existing units from various services
Institutionalization of training	SOF schoolhouses developed fairly late	Cyber schoolhouses lagging
Adequacy relative to potential demand	Desert One highlighted inadequacies in SOF	Fears of a cyber "Pearl Harbor" or other massive cyber challenge suggest that the current cyber force is inadequate to confront higher-end threat scenarios in the domain
Similarities		
Personnel	Specialized skills, equipment, and tactics; regional focus and language skills; retention difficult due to lack of career opportunities in the services; continuous and long-term development of core skills	Specialized skills, equipment, and tactics; language skills (both foreign and computer); retention difficult due to lack of career opportunities in the services and due to lucrative opportunities in the private sector; continuous and long-term development of core skills
Relationship with and to conventional forces	Cultural differences; roles and activities not well understood and differ from conventional operations	Cultural differences; roles and activities not well understood and differ from conventional operations
"Precarious values"	Mission in conflict with or in danger of being overwhelmed by primary goals of traditional military enterprise	Mission in danger of being misunderstood or ignored in pursuit of goals of traditional military enterprise
Applicability across the spectrum of conflict	Can conduct wide range of operations across the spectrum of conflict	Narrower range of operations across the spectrum of conflict
Acquisition needs	SOF-peculiar equipment, including SOF airlift; at the mercy of service budgets and priorities	Some amount of cyber-peculiar equipment needed; IA/CND dependent in part on computer acquisition choices throughout the joint force

Table 5.1—Continued

Features	Pre-USSOCOM SOF	Cyber Forces
Similarities (continued)		
Calls for reform	Services failed to meet the needs of SOF; reform suggestions included SOF as a sixth service, major command, or COCOM	Services failing to fully meet the needs of cyber forces; suggestions include cyber force as a sixth service or separate agency
Differences		
Personnel	Core capabilities as commandos; recruited entirely within services; high attrition during accession	Core capabilities in "geek arts"; best recruiting would be from civilian population; accession not as grueling
Historical tradition	Long and storied history of unconventional warriors	Relatively new capability
Salient historical events	Repeated postwar declines; reputation blackened by Vietnam; catalytic tragedy at Desert One	No iterative history; no blackened reputation; no catalytic events (no cyber "Pearl Harbor")
Core essence	Very unitary; all SOF are commandos	Unity of domain (cyberspace), but cyber forces vary in focus (i.e., defense, attack, and exploitation)

institutional advocacy and authorities) is an attractive one; the path taken to get there (embarrassment, heavy-handed congressional imposition, acrimony, and contestation) suggests the advantages of an alternative route. If possible, desired authorities should be sought consensually, without the acrimony that characterized the evolution of SOF. This may entail cautiously winning advocates at high levels in the services and on the Joint Staff. Seeking consensus and making compromises inside DoD might yield better long-term results than provocative public antagonism and angry congressional demand. In fact, the history of SOF might provide a subtle lever: If the cyber community can gather congressional allies, reference to history might persuade resisters in DoD to reach an effective compromise before Congress intervenes.

The establishment of USCYBERCOM appears to be a move in the right direction. Several of the needs of the cyber community are likely to be met by this organization. While there is some debate and concern surrounding the establishment of the command, these issues relate to the scope of its mission, its relationship to other elements of DoD, and its relationship to civilian capabilities and authorities, not the appropriateness of establishing a centralized organization, as was the case for SOF (Hodge, 2010).

The types of authorities granted to the SOF community by the Nunn-Cohen Amendment parallel many of the needs of the cyber force. The exact implementation need not match, however.

The cyber community needs advocacy. Nunn-Cohen granted SOF a four-star COCOM and an assistant secretary of defense. The cyber force would clearly benefit from such advocacy. USCYBERCOM is now commanded by GEN Keith Alexander, whose role should go a long way toward establishing institutional advocacy for the community.

The cyber community needs a joint organizational home. USSOCOM became the "home" for all SOF and the focal point of SOF advocacy. The cyber force needs a joint organizational center to foster a genuine institutional and organizational community. A home of this kind will help promote doctrine, standardized training, and the institutionalization of processes and training. USSOCOM is "service-like" in that it works as a force provider for operations run by the geographic COCOMs. The cyber force could be organized in much the same way. It is unclear to what extent USCYBERCOM in its current form will provide this kind of organizational home. While certainly a step in the right direction, it remains to be seen whether the command is a source for doctrine and training standardization. Currently, USCYBERCOM leaves far more authority for the creation and preparation of cyber forces to the services in comparison with USSOCOM's control over SOF training and development. USCYBERCOM is still a sub–unified command and not a COCOM, and the differences that implies do matter.

To the extent that the services retain organize, train, and equip responsibilities for cyber forces, these forces needs better funding support and a rapid acquisition capability. The close relationship between the NSA and USCYBERCOM promises to bring considerable resources to bear for cyber-specific tools at that level. The extent to which NSA-developed tools will intermingle with USCYBERCOM tools and the extent to which such tools will be available to the broader force remain unclear. Overreliance on the NSA, however, carries the risk of co-opting the services' Title 10 organize, train, and equip functions. It could also leave "service-retained" cyber forces without necessary tools. There must be clear decisions made with regard to the desired end states for and relationships between cyber forces in the services, joint forces, and relevant civilian agencies, including the NSA, the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and the Central Intelligence Agency. Once the desired end states are clear, it will become clear to the services which forces they need to organize, train, and equip.

For the services, the costs of equipping cyber forces with "cyber-peculiar equipment" are lower relative to the costs of procuring "SOF-peculiar equipment." The largest expense is the research and development of new tools, which might be better managed in a primarily civilian context than as part of the cumbersome DoD system acquisition process. To stay on the "bleeding edge" of technical capability, the cyber force really needs a rapid acquisition and development capability at the service level. USSOCOM has realized this agility and responsiveness in the procurement of SOF-peculiar equipment through MFP-11 using the CMNS process to develop and execute UDAs, especially where commercial solutions are available.

Even an MFP-11–like authority would not provide the cyber force with the ability to secure the network technology procured elsewhere in the joint force. That is, cyber defenders are asked to defend the network, but elements outside the cyber community continue to procure hardware and software that are not as defendable as the defenders would like. This is another instance in which advocacy and a seat at the table for the cyber community would facilitate awareness and provide a voice for these needs. Additionally, something like the "synchronizing" authority that USSOCOM holds with regard to GWOT planning across the COCOMs might be worth considering with regard to computer and network acquisition planning across the joint force.

The cyber force needs nontraditional personnel authorities. Like SOF, the cyber force needs careers, career fields, and grade structure and promotion opportunities that allow it to accomplish its mission, mature as an organization, and have high-level organic representation. Unlike SOF, the cyber force cannot reach its optimal recruitment and retention point by relying on traditional authorities. SOF could recruit its members from the ranks of conventional forces and provide the additional training needed. The cyber force cannot, because many of the skills it needs are not present in the conventional forces. The cyber force would benefit from the ability to recruit directly from the civilian workforce and innovative alternative retention incentives. There is precedent for such recruiting. Military doctors are recruited from the civilian workforce as lateral entries. The same has been true for foreign language instructors at the U.S. Military Academy. Such individuals are given rank according to their skills (cyber experts could be commissioned as warrant officers) and provided a modest amount of military training. Such provisions are not included in current plans for USCYBERCOM. As long as the services retain obligations to organize, train, and equip cyber forces, nontraditional personnel authorities should be made available to the services.

CHAPTER SIX

Lessons for U.S. Cyber Forces from U.S. Special Operations Command Acquisitions

Chapter Five made clear the similarities between SOF and the cyber force's needs to acquire unique equipment to conduct operations. For SOF, specialized vehicles and weapons may ultimately influence the outcome of a mission. Acquisition communities are dedicated to quickly delivering such equipment to the warfighter when there is an urgent need.

The speed and agility that marks the SOF acquisition process can benefit cyber acquisition. This chapter reviews the evolution of USSOCOM's acquisition program. We conclude by summarizing the factors contributing to USSOCOM's acquisition success that may be especially applicable for the cyber community.

Problems with Current Acquisition Processes

The formal DoD acquisition process is complex, consisting of many checkpoints, studies, and subprocesses. The process is designed to meet needs while satisfying all requirements, at minimum cost and risk. As a result it is notoriously slow. Specifically, defense acquisition policy (as specified in the DoD 5000-series guidance and the Joint Capabilities Integration Development System, or JCIDs) often results in program execution times—from validation of program need to fielding—on the order of ten years, or more (Bennett, 2010). Included in these acquisition efforts is the purchasing of information technology, which is also recognized as being too slow to get modern tools into the hands of warfighters. Legislation and policy changes (e.g., the Weapon System Acquisition Reform Act, National Defense Act 2010) intended to address this problem had been enacted and were in the process of being implemented as of this writing. The focus of these efforts has been on speeding up the purchasing process for IT, recognizing that the uniform method of DoD 5000-series system acquisition is too burdensome.[1]

[1] The Weapon System Acquisition Reform Act of 2009 enacted sweeping changes in DoD acquisition, including instituting new program groups in OSD (such as Cost Assessment and Program Evaluation), eliminating old positions, and instituting new legal requirements for the way in which projects are managed. It also provided an

Cyber Acquisition Needs

IT is the foundation of needed cyber assets. As described earlier, U.S. military acquisition processes are slow. Adversaries can take advantage of rapid advances in the commercial IT marketplace and thus leap ahead of DoD. In short, the United States and the Army require a cyber acquisition process that is much faster than formal DoD acquisition. This is a necessity to avoid technology obsolescence and operational disadvantages when U.S. cyber products are fielded against adversaries who have access to fast commercial processes.

When we say *cyber acquisition* what exactly are we talking about? The broadest interpretation is that cyber assets include nearly all electronic items used by the military. Cyber acquisition could (but should not) include all of these items. This is not practical or useful. For clarity, in Table 6.1, we define three levels of cyber assets based on sensitivity and specialized need.

This discussion of cyber acquisition focuses on key cyber assets of Type A and, to some extent, Type B, including tools that support CNA, CNE, CND, and situational awareness tools. As noted in Chapter Five, the choices made for acquisitions of Type C do affect the cyber force in important ways through their role in determining the defensibility of networks, but these are not the kind of assets for which expanded acquisition authorities are required.

Table 6.1
A Taxonomy of Cyber Assets

Type	Specialization	Sensitivity	Example
A	Highly specialized	Highly sensitive, designed for particular field needs	Tools associated with CNA
B	Shared across multiple missions/programs	Moderately sensitive	Fielded software/hardware (e.g., firewalls, server blades, local network backbone), commercial intrusion detection/protection systems
C	General applicability	Widely used and bulk-purchased	Office products, operating systems, laptops, printers, accessories

extensive accounting of the differences between major automated acquisition systems and major defense acquisition programs.

The National Defense Act of 2010 adopted almost all the recommendations set forth by a March 2009 Defense Science Board report on IT purchasing. The report recommended a "parallel process" for acquiring IT, stressing early prototyping, releasing small incremental improvements in capabilities on a frequent basis, and the modularity of systems. The act pushed for the elimination of ties to specific programs so that acquisitions could benefit from working capital funds appropriated according to mission need. It also advocated service-oriented architecture and an "agile" acquisition process.

Given the aforementioned and widely recognized technology acquisition problems stemming from DoD 5000-series guidance, cyber acquisition will need a different, nontraditional acquisition approach. For this reason, we undertook a study of USSOCOM's rapid acquisition process, which has been lauded as novel and successful.

U.S. Special Operations Command Rapid Acquisition Needs

USSOCOM is a "Combatant Command with legislated military department-like authorities" (USSOCOM, 2010). A primary rationale for establishing USSOCOM was the services' failure to modernize in a timely fashion the systems used for SOF operations. In 1987, Congress criticized DoD for the lack of progress in procuring "SOF-peculiar equipment" and authorized CINCSOC to function as a "head of agency" for SOF acquisition programs, an authority normally reserved for the service secretaries. The Deputy Secretary of Defense approved the establishment of the Special Operations Research, Development, and Acquisition Center (SORDAC) on December 10, 1990. In 1992, the command's acquisition and contracting management functions were consolidated into a new directorate under a deputy for acquisition, who was named the command's acquisition executive (a senior executive service position) and senior procurement executive. The forerunner to the current SORDAC was the Special Operations Acquisition and Logistics Center, which emphasized streamlined acquisition processes that included modifying existing weapons or buying nondevelopmental systems that permitted low-cost rapid improvements to provide operational capabilities, where such was possible (USSOCOM, 2002). Today, SORDAC's charter has expanded to include procurement of new systems for USSOCOM where no suitable system is available or in development elsewhere.

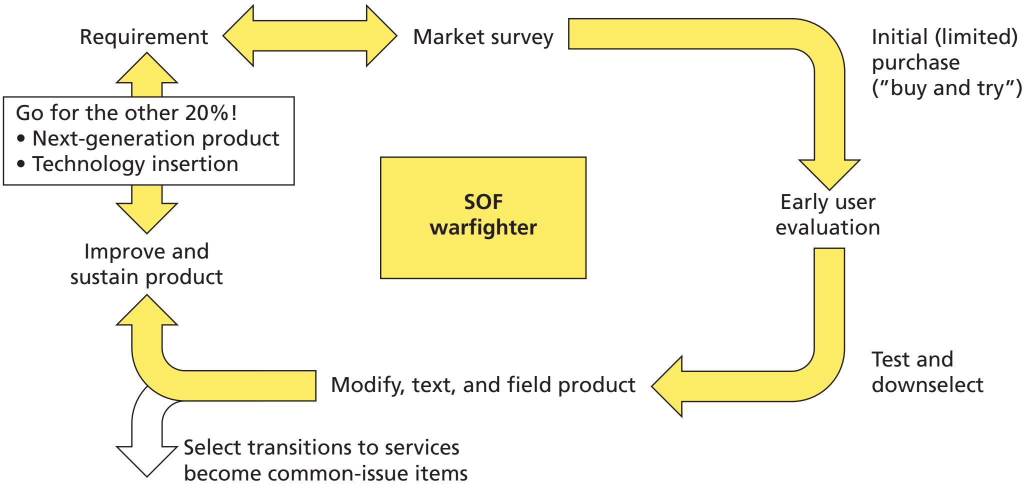
U.S. Special Operations Command Rapid Acquisition Processes

USSOCOM has streamlined the formal DoD acquisition process for its urgently needed capabilities, as shown in Figure 6.1. This is allowed because, under conditions of urgent need, exceptions to the formal DoD acquisition process are permitted.[2] USSOCOM describes it as an "80-percent solution" process (Uhler, 2004).

> USSOCOM developed an urgent deployment acquisition process to provide rapid acquisition and logistics support in response to combat mission needs statements from deployed SOF and those about to deploy. The command has acquired and fielded advanced technology systems in as little as seven days once the combat

[2] Joint doctrine states that "compliance with JCIDS is not required to support fielding of an immediate solution to an urgent war fighting need" (see CJCSI 3170.01E, 2005).

Figure 6.1
U.S. Special Operations Command Rapid Acquisition Features


Requirement
Market survey
Initial (limited) purchase ("buy and try")
Go for the other 20%!
• Next-generation product
• Technology insertion
SOF warfighter
Early user evaluation
Improve and sustain product
Test and downselect
Modify, text, and field product
Select transitions to services become common-issue items

SOURCE: Uhler, 2004, slide 4.

NOTE: According to regulations, follow-up compliance is required for long-term solutions (Center for Program Management, Defense Acquisition University, 2005.

RAND *MG1132-6.1*

> mission needs statement was approved, and most capabilities were delivered in less than six months. The accelerated acquisition process produced mobile electronic-warfare jammers, target video downlink capabilities for close air support aircraft, anti-structural grenades, and unmanned aerial systems. (USSCOM, 2007, p. 24)

Culture and Other Keys to Success

USSOCOM sustains a rapid acquisition culture that begins with self-contained management, system engineering, contracting, logistics, and test teams. This culture of independence, self-reliance, and pride in performance depends on small, focused teams using (in order of preference) government, commercial, or modified government or commercial products to satisfy urgent requirements. It uses the formal acquisition process only as a last resort. The teams work closely with warfighters and contractors. USSOCOM's rapid acquisition approach is expedited in three important ways.

Quick Recognition and Validation

USSOCOM's rapid acquisition program begins with the determination of a validated need, often in a matter days. This step can take many months in the formal acquisition process.

Deployed SOF, including deployed SORDAC teams, notify SORDAC about capability gaps. The needs validated by SORDAC are addressed through one of three processes, depending on the type of gap and the ability to close it: CMNS and the UDA process, the Joint Acquisition Task Force approach, or the SOF Capability Integration Development System process.

CMNS acquisitions have the highest priority and trigger the UDA process. The distinguishing characteristic of these needs is that, if not met, they will likely result in serious loss of SOF lives. Validated CMNS capabilities are provided by the acquisition center within 25 days of gap recognition. Fielding is required within 180 days, and a program memorandum is immediately assigned. The most streamlined of procedures are employed, including the highest defense priority rating, an abbreviated SORDAC acquisition management plan, an immediate waiver of JCIDS, and expedited fielding, including initial fielding and conditional fielding and deployment. Sustainment is ordinarily required for only one year. The process relies on intense management coordination, including monthly or more frequent USSOCOM management reviews and immediate notification of the USSOCOM acquisition executive of any impediments that arise over the course of implementation. Central to the CMNS/UDA process is a rapid-response team.[3] According to USSOCOM (2010), this is a lean, subject-matter expert group colocated with USSOCOM staff. The abbreviated process seeks to limit the time between an SOF-submitted CMNS and acquisition action to 25 days or less. Currently, $2 million is set aside annually for UDA.

Joint acquisition task forces were first created in 2009 to deal with more complex UDA capabilities that could be fielded in less than one year. The program statement of work is divided into major subtasks assigned to task force teams. This approach was successfully applied to project Dragon Spear, a program to create a variant of the C-130 gunship using off-the-shelf sensors, communication systems, guided missiles, and a light caliber gun integrated into a non-gunship C-130 for SOF use. Teams were assigned along the aforementioned lines to expedite delivery. The first aircraft was delivered for predeployment training in ten months, with first deployment to the field expected ahead of schedule. The task forces are disbanded when their work is finished, and a more traditional management structure continues the program.

Special Operations Capabilities Integration Development System programs, like the first two discussed, use that system in place of JCIDS. The approach is faster and more streamlined than JCIDS. Such programs are typically completed in less than two years.[4]

[3] The team includes the deputy commander (for approval), the J2/J3 (for certification), the J8 (for validation), the J8-R (to serve as rapid-response team lead), the J codes (J4, J6, J7, J9), assessment directors (J8-A), test and evaluation personnel (J8-O), SORDAC, the Office of the Director of Special Operations Financial Management and Comptroller, the theater special operations component, the endorsing USSOCOM component (USSOCOM, 2010).

[4] In addition to these, of course, SORDAC has longer-term programs, including the Acquisition Category I and II programs.

The Ability to Contract to Develop Products Quickly

USSOCOM's acquisition process continues with the rapid award of a directed contract to one or more contractors chosen from those with indefinite delivery/indefinite quantity (IDIQ) contracts to expedite procurement. The approach uses streamlined contract provisions to eliminate all but the essential steps necessary to deliver the products. Product testing is also accelerated by the use of USSOCOM's in-house test organization.

The Ability to Equip Selected Warfighters Rather Than Field Capabilities to the Entire Force

Following a successful test, the product is supplied to warfighters, at times in less than 180 days from the identification of its need. SORDAC has its own contracting staff, program management staff, test organization, and acquisition authority that—along with a rapid acquisition philosophy and dedication—expedite the acquisition process. Selected warfighters are equipped quickly, because of the emphasis on their unique mission needs. This prioritization differs from the goals of the greater acquisition community, which must concentrate on fielding capabilities to the entire force.

Track Record of U.S. Special Operations Command's Rapid Acquisition Programs

The U.S. Government Accountability Office reviewed SORDAC's programs in 2007, concluding that 60 percent of USSOCOM acquisition programs undertaken since 2001 have progressed as planned, staying within their original cost and schedule estimates (GAO, 2007). Forty percent have not progressed as planned and experienced modest to (in a small number of cases) significant cost increases and schedule delays because of a range of technical and programmatic issues. In contrast, more than 50 percent of DoD's major defense acquisition programs do not meet cost goals, and fully 80 percent experience an increase in unit cost from initial estimates (GAO, 2011).

As of 2007, USSOCOM had delivered 97 discrete systems for OIF and OEF in response to CMNS requests, including mobile electronic warfare jammers, target video downlink capabilities for close air support aircraft, anti-structural grenades, and remotely piloted aircraft (USSOCOM, 2007).

Clearly, USSOCOM has been successful in the programs that it manages directly, many of which are in the rapid acquisition categories. In fact, the Army accelerated its rapid acquisition process after 9/11 and modeled its procedures after those used by USSOCOM ("RAND/Members of the Army Rapid Equipping Force," 2010).

How Cyber Acquisition Could Be Modeled After the U.S. Special Operations Command Rapid Acquisition Approach

Many cyber technologies and products have fast development and deployment cycles that must be matched with rapid acquisition processes to avoid obsolescence when deployed. USSOCOM's rapid acquisition success should be exploited to enhance cyber acquisition success.

In this section, we present 17 lessons drawn from USSOCOM acquisition experience that have relevance for cyber acquisitions. Note that the first two lessons would require major, revolutionary changes to current service acquisition processes and regulations; the remaining 15 are still useful but would require less dramatic reforms.

1. Obtain unique, self-contained acquisition authority, equivalent to that provided to the military services.
2. Have your own budget.
3. Seek authority to streamline for urgent needs in a manner consistent with DoD 5000-series and JCIDS provisions. This authority should be used more dramatically than it is by the services, based on the urgent and extreme nature of the missions and comparatively small quantity and short life required for fielded capabilities.
4. Employ self-contained program management, contracting, system engineering, testing, and training capabilities.
5. Inculcate a "yes-culture"; for example, only the USSOCOM commander and the USSOCOM acquisition executive can say no to meeting a validated urgent need.
6. Keep the acquisition organization as small as is practical. Use small, centralized, frequently colocated management teams.
7. Minimize bureaucracy and paperwork and employ short chains of command.
8. Avoid fieldings. Focus on equipping. According to the Army Rapid Equipping Force organization, fielding is a complete and detailed DOTMLPF approach focused on a general solution for the entire Army. Equipping is a timely and evolvable rapid solution that meets or exceeds minimum DOTMLPF requirements and focuses on the needs of a specific unit or theater. Equipping meets the specialized needs of a few units; fielding is for the entire Army and is more appropriate for Acquisition Category I or II procurement.
9. Focus on relatively small-scale, short-cycle programs (e.g., avoid Acquisition Category I or II programs).
10. Accept informed risk and accept consequent failure when it occurs.
11. Accept the 70- to 80-percent solution; deferring the missing 30–20 percent to the next-generation product.

12. Where applicable, give preference to commercial, off-the-shelf, or government, off-the-shelf products and nondevelopmental items. Pursue new development only when necessary.
13. Use demonstrated, capable contractors placed on IDIQ contracts whose support can be mobilized quickly.
14. Use meaningful metrics through competitive prototyping and define real operational envelopes in this way.
15. Manage expectations; the primary obstacles are policy and culture, not technology. Focus on the user/business benefit, not the technical capability.
16. Constantly engage with industry and academe to maintain awareness of the art (or the state of the possible).
17. Maintain a constant presence—with units in the field, with potential customers, with Network Enterprise Centers, and with industry and military labs (e.g., the Air Force Research Laboratory, the Navy's Space and Naval Warfare Systems Command, the Army's Communications-Electronics Research, Development, and Engineering Center).

Summary

JCIDS allows exceptions for urgent needs, and USSOCCOM has been successful in using them. The USSOCOM approach is guided by the following objectives:

- Clearly communicate the warfighter's need.
- Understand the underlying intent.
- Search for readily available solutions: service-common, commercial, or non-developmental.
- Accept a managed risk.
- Quickly flag issues.
- Facilitate fast user evaluation.
- Let the warfighter know of limits and concerns.
- Field initial capability within 180 days.
- Be transparent: Provide quarterly financial reporting to OSD or Congress, as applicable.

Overall, the USSOCOM acquisition organization has been a pioneer guided by a set of general rules: (1) stay small but aware, (2) reduce paperwork and avoid over-specifying requirements, and (3) work fast and do not be afraid to take (informed) risks. Cyber acquisition should be modeled after USSOCOM's rapid acquisition approach to the extent possible.

CHAPTER SEVEN

Conclusions and Recommendations

This monograph described the history of the formation of USSOCOM, discussed similarities and differences between early SOF and contemporary cyber forces, and presented an analogy between the two. Given the similarities between the two communities, the path to and authorities held by USSOCOM suggest several lessons for the growth and evolution of the U.S. cyber force. Specifically, like earlier SOF, the cyber community needs advocacy and a joint organizational home. Similar to pre-USSOCOM SOF, it needs *better funding support* and *a rapid acquisition capability*. However, it is much more dependent on technical acquisition choices at the joint force level. In contrast to SOF, the cyber force needs *nontraditional personnel authorities*.

The establishment of USCYBERCOM promises to address some of these needs, in whole or in part. Specifically, USCYBERCOM should contribute significantly toward the resolution of the first two needs, institutionalized senior advocacy and a joint home. USCYBERCOM in its current incarnation is as a subordinate unified command under USSTRATCOM, and it does not include any new acquisition or personnel authorities, so further efforts may be necessary to address the final two needs (a rapid acquisition capability and nontraditional personnel authorities).

The success of USCYBERCOM will hinge on the support of the services, since service-level cyber organizations will contribute both equipment and personnel. The future of the cyber community will hinge, to some extent, on the evolving relationship between USCYBERCOM and the services. Implementation lessons from the early days of USSOCOM suggest that such cooperation and support should not be taken for granted. USCYBERCOM should hope for good-faith support from the services and their representatives but be explicit about exactly what is required and be prepared for bureaucratic disputes.

Based on these findings and on uncertainty about what exactly USCYBERCOM will ultimately look like, we make two sets of recommendations, one for the broader DoD cyber community and a second for the U.S. Army cyber community specifically.

Recommendations for the U.S. Department of Defense

Empower USCYBERCOM as a Joint Home for the Cyber Community.

Seek to develop USCYBERCOM as more than just the operational organization for the coordination of operations in cyberspace. It can also serve as an organization *for the coordination, management, and professionalization of all DoD cyber forces*. It should have authority over schoolhouses and the development of training standards, as well as influence over the career paths of cyber personnel.

Find Acquisition Solutions for Needed Cyber Tools

This monograph is agnostic as to whether these authorities should be at the joint level (USCYBERCOM) or at the service level, but cyber forces need rapid acquisition capabilities like those employed by USSOCOM.

Recommendations for the U.S. Army

Support USCYBERCOM as a Capstone Coordinator of and Organizational Home for the Entire Cyber Force

Rather than viewing USCYBERCOM as an imposition or as a poacher of valuable cyber personnel, recognize (and encourage) USCYBERCOM as a central source of operational experience, training standards, career progression options, and capability development. If USCYBERCOM matures to have many of the beneficial features of USSOCOM identified in this monograph, then what is good for USCYBERCOM will be good for Army cyber forces and will be good for U.S. cyber forces more broadly.

Make U.S. Army Cyber Command for the Army's Cyber Forces What USSOCOM Is for All SOF

Empower Army Cyber Command as the institutional home for Army cyber forces and as the seat of advocacy within the Army. Empower it to develop clear career trajectories for Army cyber forces; ensure that these plans support the needs of USCYBERCOM and correspond with the training standardization and career authorities that develop at USCYBERCOM. The relationship between USASOC and USSOCOM might be a good template for a relationship between Army Cyber Command and USCYBERCOM.

Recognize the Precarious Value of Cyber Forces and Support Them Accordingly

One of the lessons from the history of SOF applies to all of the services: To retain control over a precarious value, it is imperative to demonstrate a commitment to the health and well-being of that value. That means maintaining resource priority, effective advocacy, and committed force development for Army cyber forces. This requires, first and foremost, commitment to the capability on the part of leadership.

Reform Army Cyber Acquisition

Cyber forces need a rapid and flexible ability to acquire cyber-specific tools. As the Title 10 organize, train, and equip authority, the Army should seek this capability for Army cyber forces. In addition, reforms to the way in which IT is acquired Army-wide should be pursued to reduce the difficulty of IA and the burden on cyber defenders.

Seek Nontraditional Personnel Authorities

Unlike SOF, the best pool of potential cyber recruits can be found in the civilian workforce. The characteristics of optimal cyber recruits differ, however, from the characteristics of traditional Army recruiting targets. New and different authorities for cyber force recruiting and management could substantially improve the Army's ability to generate and maintain cyber forces.

Model Cyber Acquisition After USSOCOM's Rapid Acquisition Approach

Overall, USSOCOM's acquisition organization has been a pioneer guided by a set of general rules: (1) stay small but aware, (2) reduce paperwork and avoid overspecifying requirements, and (3) work fast and do not be afraid to take (informed) risks.

References

Abbott, Andrew, "Conceptions of Time and Events in Social Science Methods: Causal and Narrative Approaches," *Historical Methods*, Vol. 23, No. 4, 1990, pp. 140–150.

Aminzade, Ronald, "Historical Sociology and Time," *Sociological Methods and Research*, Vol. 20, No. 4, May 1992, pp. 456–480.

Anderson, Steven C., *Equipping the Air Commando: The Procurement of Commercial Derivative Aircraft for Air Force Special Operations Command*, Maxwell AFB, Ala.: Air Command and Staff College, Air University, April 2008.

Andures, Wesley R., "What U.S. Cyber Command Must Do," *Joint Force Quarterly*, No. 59, 4th Quarter, 2010, pp. 115–120.

Armistead, Leigh, ed., *Information Operations: Warfare and the Hard Reality of Soft Power*, Washington, D.C.: Brassey's, 2004.

Bennett, John T., "Gates: Speed FCS Replacement, Define Future USMC Role," *DefenseNews*, May 7, 2010. As of July 7, 2014:
http://www.defensenews.com/story.php?i=4617217

Berinato, Scott, "The Future of Security," *Computerworld*, December 30, 2003. As of July 7, 2014:
http://www.computerworld.com/printthis/2003/0,4814,88646,00.html

Birdwell, M. Bodine, and Robert Mills, "War Fighting in Cyberspace: Evolving Force Presentation and Command and Control," *Air and Space Power Journal*, Spring 2011, pp. 26–36.

Bowdan, Mark, "The Desert One Debacle," *Atlantic Magazine*, May 2006. As of July 7, 2014:
http://www.theatlantic.com/doc/200605/iran-hostage

Boykin, William G., *The Origins of the United States Special Operations Command*, Carlisle, Pa., undated.

Carden, Michael J., "Official Cites Need for Technology Acquisition Reform," American Forces Press Service, July 10, 2009. As of July 7, 2014:
http://www.defense.gov/news/newsarticle.aspx?id=55083

Center for Program Management, Defense Acquisition University, "Joint Capabilities Integration and Development System," briefing, May 2005.

Chairman of the Joint Chiefs of Staff Instruction 3170.01E, Joint Capabilities Integration and Development System, May 11, 2005.

CJCSI—*See* Chairman of the Joint Chiefs of Staff Instruction.

Cluck, James, director, Center for Acquisition and Logistics, U.S. Special Operations Command, "USSOCOM Acquisition Perspective to NDIA," briefing, March 20, 2009, As of November 4, 2011: http://www.ndia-cfl.org/news/defense_forum/2009/SOAL_NDIA_20Mar09v2.pptx

Conti, Gregory, and John Surdu, "Army, Navy, Air Force, and Cyber—Is It Time for a Cyberwarfare Branch of Military?" *IAnewsletter*, Vol. 12, No. 1, Spring 2009.

Daniel, Dan, "U.S. Special Operations: The Case for a Sixth Service," *Armed Forces Journal International*, August 1985, pp. 71–75.

DoD—*See* U.S. Department of Defense.

Doty, Joseph, and T. J. O'Connor, "Building Teams of Cyber Warriors," *Army Magazine*, January 2010, pp. 12–14.

GAO—*See* U.S. Government Accountability Office.

Hodge, Nathan, "Prospective U.S. Cyber Commander Talks Terms of Digital Warfare," *Wired*, April 15, 2010. As of July 7, 2014:
http://www.wired.com/dangerroom/2010/04/pentagons-prospective-cyber-commander-talks-terms-of-digital-warfare

Jackson, William, "DoD Creates Cyber Command as U.S. Strategic Command Subunit," *Federal Computer Week*, June 24, 2009.

Kessler, Carrie L., "39 IOS Unveils Advanced Cyber Schoolhouse Addition," U.S. Air Force Special Operations Command, July 27, 2010. As of July 7, 2014:
http://www.afsoc.af.mil/news/story.asp?id=123215117

Khong, Yuen Foong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965*, Princeton, N.J.: Princeton University Press, 1992.

Lenahan, Rod, *Crippled Eagle: A Historical Perspective of U.S. Special Operations, 1976–1996*, Charleston, S.C.: Narwhal Press, 1998.

Lord, William T. "AFCYBER (P) Commander Bids Farewell to Troops," U.S. Air Force Cyber Command, July 10, 2009.

Marquis, Susan L., *Unconventional Warfare: Rebuilding U.S. Special Operations Forces*, Washington, D.C.: Brookings Institution Press, 1997.

Martinage, Robert, "Special Operations Forces: Challenges and Opportunities," testimony before the U.S. House of Representatives Committee on Armed Services, Subcommittee on Terrorism, Unconventional Threats and Capabilities, Washington, D.C., March 3, 2009.

McKaughan, Jeff, "Q&A: James W. Cluck," *Special Operations Technology*, Vol. 7, No. 4, June 2009.

Moorehead, Col. Rich, U.S. Air Force, interview with the authors, RAND Corporation, Santa Monica, Calif., February 10, 2010.

National Security Agency/Central Security Service, "Mission," web page, last updated April 15, 2011. As of July 7, 2014:
http://www.nsa.gov/about/mission/index.shtml

NSA/CSS—*See* National Security Agency/Central Security Service.

Olson, Eric T., "Statement of Admiral Olson Before the Senate Armed Services Committee on the Posture of Special Operations Forces," transcript, Washington, D.C., March 4, 2008.

Paul, Christopher, *Marines on the Beach: The Politics of U.S. Military Intervention Decision Making*, Westport, Conn.: Praeger Security International, 2008.

Peters, John E., and James A. Dewar, *A Vision for USSOCOM*, unpublished RAND research, June 1998.

Porche, Isaac R. III, Bruce J. Held, Jerry M. Sollinger, Timothy M. Bonds, Ian P. Cook, Bradley Wilson, R. Wayne Dudding, and Christopher Paul, *The Army's Role in Cyberspace*, unpublished RAND research, 2008.

Porche, Isaac R. III, Christopher Paul, Elliot Axelband, Jerry M. Solinger, Bruce J. Held, Bradley Wilson, Ian P. Cook, Michelle Kam, and R. Wayne Dudding, *Developing Army Capabilities for Cyber-Operations*, unpublished RAND research, September 2010.

Public Law 100-180, National Defense Authorization Act for Fiscal Years 1988 and 1989, December 4, 1987.

Public Law 100-456, National Defense Authorization Act for Fiscal Year 1989, September 29, 1988.

Pyburn, Bradley L., *Application of U.S. Special Operations Command Model to Department of Defense Cyberspace Force*, Quantico, Va.: U.S. Marine Corps Command and Staff College, 2009.

"RAND/Members of the Army Rapid Equipping Force," meeting notes, April 14, 2010.

Record, Jeffrey, *Perils of Reasoning by Historical Analogy: Munich, Vietnam, and American Use of Force Since 1945*, Maxwell AFB, Ala.: Center for Strategy and Technology Air War College, Occasional Paper No. 4, March 1998.

Shachtman, Noah, "Air Force Suspends Controversial Cyber Command," *Wired*, August 13, 2008. As of July 7, 2014:
http://www.wired.com/dangerroom/2008/08/air-force-suspe

Starr, Stuart, Daniel Kuehl, and Terry Pudas, "Perspectives on Building a Cyber Force Structure," in Christian Czosseck and Karlis Podins, eds., *Conference on Cyber Conflict Proceedings 2010*, Tallinn, Estonia: CCD COE Publications, 2010, pp. 163–181.

Stewart, Richard W., *Sine Pari: Without Equal: The Story of Army Special Operations*, Ft. Bragg, N.C.: U.S. Army Special Operations Command, Directorate of History and Museums, 1997.

Stewart, Richard W., Stanley L. Sandler, and Joseph R. Fischer, *Command History of the United States Army Special Operations Command, 1987–1982: Standing Up the MACOM*, Ft. Bragg, N.C.: U.S. Army Special Operations Command, Directorate of History and Museums, 1996.

Stryker, Robin, "Beyond History Versus Theory: Strategic Narrative and Sociological Explanation," *Sociological Methods and Research*, Vol. 24, No. 3, February 1996, pp. 304–352.

Uhler, D. G., acquisition executive, U.S. Special Operations Command, "Revitalizing System Engineering: US Special Operations Command Approach," briefing, November 16, 2004.

U.S. Army, "Army Establishes Army Cyber Command," October 1, 2010. As of July 7, 2014:
http://www.army.mil/-news/2010/10/01/46012-army-establishes-army-cyber-command

———, "Army Cyber Command," information paper accompanying *2011 U.S. Army Posture Statement*, Washington, D.C., March 2011.

U.S. Department of Defense, "Cyber Command Achieves Full Operational Capability," press release, Washington, D.C., No. 1012-10, November 3, 2010a.

———, "U.S. Cyber Command Fact Sheet," Washington, D.C., May 25, 2010b.

U.S. Department of Homeland Security, *Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development*, Washington, D.C., September 2008.

U.S. Government Accountability Office, *Defense Acquisitions: An Analysis of the Special Operations Command's Management of Weapon System Programs*, Washington, D.C., GAO-07-620, June 2007.

———, *Defense Acquisitions: Assessments of Selected Weapon Programs*, Washington, D.C., GAO-11-233SP, March 2011.

U.S. Navy Center for Information Dominance, "Mission," web page, undated. As of July 7, 2014: https://www.netc.navy.mil/centers/ceninfodom/CommandInfo.aspx?ID=1

U.S. Senate, Committee on Armed Services, "Nominations of VADM James A. Winnefeld, Jr., USN, to Be Admiral and Commander, U.S. Northern Command/Commander, North American Aerospace Defense Command; and LTG Keith B. Alexander, USA, to Be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command," hearing transcript, Washington, D.C., April 15, 2010.

USSOCOM—*See* U.S. Special Operations Command.

U.S. Special Operations Command, Special Operations in Peace and War, MacDill AFB, Fla., January 25, 1996.

———, *History*, 15th anniversary ed., MacDill AFB, 2002.

———, *Posture Statement 2003–2004: Transforming the Force at the Forefront of the War on Terrorism*, 2003.

———, *History*, 20th anniversary ed., MacDill AFB, 2007.

———, *History*, 6th ed., MacDill AFB, Fla., 2008.

———, "Briefing to RAND," briefing, May 23, 2010.

With the establishment of U.S. Cyber Command in 2010, the cyber force is gaining visibility and authority, but challenges remain, particularly in the areas of acquisition and personnel recruitment and career progression. A review of commonalities, similarities, and differences between the still-nascent U.S. cyber force and early U.S. special operations forces, conducted in 2010, offers salient lessons for the future direction of U.S. cyber forces. Although U.S. special operations forces (SOF) have a long and storied history and now represent a mature, long-standing capability, they struggled in the 1970s and 1980s before winning an institutional champion and joint home in the form of U.S. Special Operations Command. U.S. cyber forces similarly represent a new but critical set of military capabilities. Both SOF and cyber forces are, at their operating core, small teams of highly skilled specialists, and both communities value skilled personnel above all else. Irregular warfare and SOF doctrine lagged operational activities, and the same is true of the cyber force. Early SOF, like the contemporary cyber force, lacked organizational cohesion, a unified development strategy, and institutionalized training. Perhaps most importantly, the capabilities of both forces have traditionally been inadequate to meet demand. The analogy holds for issues of acquisition, the two forces' relationship with the conventional military, their applicability across the spectrum of combat, and their historic need for a strong advocate for reform. The analogy is not perfect, however. In terms of core capabilities, force accession, and tradition, the forces are also very different. But even these differences offer fundamental lessons for both the U.S. Department of Defense and the U.S. Army with regard to the future and potential of the cyber force.

RAND ARROYO CENTER

www.rand.org

$21.00

ISBN-10 0-8330-5973-4
ISBN-13 978-0-8330-5973-4

52100

9 780833 059734

RR-780-A